OWASP TOP 10 2021

Description

The primary aim of the OWASP Top 10 is to educate developers, designers, architects, managers, and organizations about the consequences of the most important web application security weaknesses. The Top 10 provides basic techniques to protect against these high risk problem areas - and also provides guidance on where to go from here.

Disclaimer

This document or any of its content cannot account for, or be included in any form of legal advice. The outcome of a vulnerability scan (or security evaluation) should be utilized to ensure that diligent measures are taken to lower the risk of potential exploits carried out to compromise data.

Legal advice must be supplied according to its legal context. All laws and the environments in which they are applied, are constantly changed and revised. Therefore no information provided in this document may ever be used as an alternative to a qualified legal body or representative.

A portion of this report is taken from OWASP's Top Ten 2021 Project document, that can be found at http://www.owasp.org.

Scan Detail

Target	http://10.255.112.211/
Scan Type	Full Scan
Start Time	Nov 11, 2025, 3:21:10 PM GMT
Scan Duration	4 minutes
Requests	18300
Average Response Time	3ms
Maximum Response Time	20002ms
Application Build	v24.6.240626115
Authentication Profile	-

Compliance at a Glance

CATEGORY	
28	A01 Broken Access Control
8	A02 Cryptographic Failures
20	A03 Injection
7	A04 Insecure Design
11	A05 Security Misconfiguration
87	A06 Vulnerable and Outdated Components
9	A07 Identification and Authentication Failures
8	A08 Software and Data Integrity Failures
0	A09 Security Logging and Monitoring Failures
4	A10 Server-Side Request Forgery

Detailed Compliance Report by Category

This section is a detailed report that explains each vulnerability found according to individual compliance categories.

A01 Broken Access Control

Access control enforces policy such that users cannot act outside of their intended permissions. Failures typically lead to unauthorized information disclosure, modification, or destruction of all data or performing a business function outside the user's limits.

WordPress XML-RPC authentication brute force

WordPress provides an XML-RPC interface via the xmlrpc.php script. XML-RPC is remote procedure calling using HTTP as the transport and XML as the encoding. An attacker can abuse this interface to brute force authentication credentials using API calls such as **wp.getUsersBlogs**.

CWE
CWE-521

CVSS2
AV:N/AC:L/Au:N/C:P/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	None
Availability Impact	None

CVSS3
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:N/A:N

Base Score	5.8
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Changed
Confidentiality	Low
Integrity Impact	None
Availability Impact	None

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N

Base Score	6.9
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	None
Confidentiality Impact to the Vulnerable System	Low
Integrity Impact to the Vulnerable System	None
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

An attacker can brute force the authentication credentials for your WordPress blog.

http://10.255.112.211/xmlrpc.php

Pattern found:

```
<value><string>Incorrect username or password.</string></value>
```

Request

```
POST //xmlrpc.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Cookie: wordpress_test_cookie=WP+Cookie+check
Content-Length: 264
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0 Safari/537.36
Host: 10.255.112.211
Connection: Keep-alive

<?xml version="1.0" encoding="iso-8859-1"?>
<methodCall>
<methodName>wp.getUsersBlogs</methodName>
<params>
<param><value><string>admin</string></value></param>
<param><value><string>8947589543789543753498 7</string></value>
</param>
</params>
</methodCall>
```

Recommendation

It is possible to disable the XML-RPC script if you do not want to use it. Consult references for a WordPress plugin that does that. If you don't want to disable XML-RPC you can monitor for XML-RPC authentication failures with a Web Application Firewall like ModSecurity.

References

WordPress XML-RPC Brute Force Scanning
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/honeypot-alert-wordpress-xml-rpc-brute-force-scanning/

Prevent XMLRPC
https://wordpress.org/plugins/prevent-xmlrpc/

WordPress brute force attack via wp.getUsersBlogs
https://isc.sans.edu/diary/+WordPress+brute+force+attack+via+wp.getUsersBlogs/18427

WordPress 5.1.x Multiple Vulnerabilities

WordPress is prone to multiple vulnerabilities, including cross-site scripting, cross-site request forgery and directory traversal vulnerabilities. Exploiting these issues could allow an attacker to execute arbitrary script code in the browser of an unsuspecting user in the context of the affected site, allowing the attacker to steal cookie-based authentication credentials, to perform certain administrative actions and gain unauthorized access to the affected application, or to obtain sensitive information that may help in launching further attacks. WordPress versions 5.1.x ranging from 5.1 and up to (and including) 5.1.15 are vulnerable.

CWE
CWE-862

CVSS2
AV:N/AC:L/Au:N/C:P/I:P/A:N/E:H/RL:OF/RC:C

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	Partial
Availability Impact	None
Exploitability	High
Remediation Level	Official Fix
Report Confidence	Confirmed

CVSS3
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N

Base Score	6.5
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity Impact	Low
Availability Impact	None

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:N/SC:N/SI:N/

Base Score	6.9
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	None
Confidentiality Impact to the Vulnerable System	Low
Integrity Impact to the Vulnerable System	Low
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

http://10.255.112.211/
wordpress v5.1.1-5.1.1

http://10.255.112.211/
wordpress v5.1.1-5.1.1

http://10.255.112.211/
wordpress v5.1.1-5.1.1

http://10.255.112.211/
wordpress v5.1.1-5.1.1

http://10.255.112.211/
wordpress v5.1.1-5.1.1

http://10.255.112.211/

wordpress v5.1.1-5.1.1

http://10.255.112.211/

wordpress v5.1.1-5.1.1

http://10.255.112.211/

wordpress v5.1.1-5.1.1

http://10.255.112.211/

wordpress v5.1.1-5.1.1

http://10.255.112.211/

wordpress v5.1.1-5.1.1

Recommendation

Update to WordPress version 5.1.16 or latest

References

https://patchstack.com/articles/wordpress-core-6-2-1-security-update-technical-advisory/
https://patchstack.com/articles/wordpress-core-6-2-1-security-update-technical-advisory/

https://www.wordfence.com/blog/2023/05/wordpress-core-6-2-1-security-maintenance-release-what-you-need-to-know/
https://www.wordfence.com/blog/2023/05/wordpress-core-6-2-1-security-maintenance-release-what-you-need-to-know/

https://wordpress.org/news/2023/05/wordpress-6-2-1-maintenance-security-release/
https://wordpress.org/news/2023/05/wordpress-6-2-1-maintenance-security-release/

WordPress Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') Vulnerability

WordPress Core is vulnerable to Directory Traversal in versions up to, and including, 6.2, via the 'wp_lang' parameter. This allows unauthenticated attackers to access and load arbitrary translation files. In cases where an attacker is able to upload a crafted translation file onto the site, such as via an upload form, this could be also used to perform a Cross-Site Scripting attack.

CWE
CWE-22

CVSS3
CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

Base Score	6.1
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	Required
Scope	Changed
Confidentiality	Low
Integrity Impact	Low
Availability Impact	None

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:L/SI:L/SA:N

Base Score	5.1
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	Active
Confidentiality Impact to the Vulnerable System	None
Integrity Impact to the Vulnerable System	None
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	Low
Integrity Impact to the Subsequent System	Low
Availability Impact to the Subsequent System	None

Impact

http://10.255.112.211/

wordpress v5.1.1-5.1.1

http://10.255.112.211/

wordpress v5.1.1-5.1.1

References

CVE-2023-2745
https://nvd.nist.gov/vuln/detail/CVE-2023-2745

WordPress Exposure of Sensitive Information to an Unauthorized Actor Vulnerability

Wordpress is an open source CMS. One of the blocks in the WordPress editor can be exploited in a way that exposes password-protected posts and pages. This requires at least contributor privileges. This has been patched in WordPress 5.7.1, along with the older affected versions via minor releases. It's strongly recommended that you keep auto-updates enabled to receive the fix.

CWE
CWE-200

CVSS3
CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N

Base Score	4.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	Low
User Interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity Impact	None
Availability Impact	None

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	Low
User Interaction	None
Confidentiality Impact to the Vulnerable System	Low
Integrity Impact to the Vulnerable System	None
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

http://10.255.112.211/

wordpress v5.1.1-5.1.1

http://10.255.112.211/

wordpress v5.1.1-5.1.1

References

CVE-2021-29450
https://nvd.nist.gov/vuln/detail/CVE-2021-29450

WordPress username enumeration

If permalinks are enabled, in many WordPress installations it is possible to enumerate all the WordPress usernames iterating through the author archives. Whenever a post is published, the username or alias is shown as the author. For example, the URL http://site.com/?author=1 will show all the posts from user id 1. Attackers can abuse this functionality to figure out which usernames are available on the site.

CWE
CWE-200

CVSS2
AV:N/AC:L/Au:N/C:P/I:N/A:N

Access Vector	Network

CVSS3
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Base Score	5.3

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:P/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N

Base Score	5.3

Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	None
Availability Impact	None

Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity Impact	None
Availability Impact	None

Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	Passive
Confidentiality Impact to the Vulnerable System	Low
Integrity Impact to the Vulnerable System	None
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

An attacker can enumerate the WordPress usernames and use this information to conduct brute-force attacks against passwords for these known usernames.

http://10.255.112.211/

List of WordPress users for {'_nativeUrl': {'password': '', 'username': '', 'search': '', 'protocol': 'http', 'port': '', 'path': '/', 'origin': 'http://10.255.112.211', 'href': 'http://10.255.112.211/', 'hostname': '10.255.112.211', 'host': '10.255.112.211', 'hash': ''}}:

['admin']

Request

```
POST //wp-login.php HTTP/1.1
Content-type: application/x-www-form-urlencoded
Cookie: wordpress_test_cookie=WP+Cookie+check
Content-Length: 28
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0 Safari/537.36
Host: 10.255.112.211
Connection: Keep-alive

log=10&pwd=z&wp-submit=Login
```

Recommendation

You can use an .htaccess rewrite rule to prevent this disclosure but you should also be sure to use nicknames to avoid disclosing usernames.

```
# Stop WordPress username enumeration vulnerability
RewriteCond %{REQUEST_URI} ^/$
RewriteCond %{QUERY_STRING} ^/?author=([0-9]*)
RewriteRule ^(.*)$ http://yoursite.com/somepage/? [L,R=301]
```

Possible sensitive directories

One or more possibly sensitive directories were found. These resources are not directly linked from the website. This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.

CWE

CWE-200

CVSS2

AV:N/AC:L/Au:N/C:P/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	None

CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	Low

CVSS4

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N

Base Score	6.9
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	None
Confidentiality Impact to the Vulnerable System	Low

Availability Impact	None

Integrity Impact	None
Availability Impact	None

Integrity Impact to the Vulnerable System	None
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

These directories may expose sensitive information that could help a malicious user to prepare more advanced attacks.

http://10.255.112.211/

Possible sensitive directories:

- http://10.255.112.211/wp-admin/**includes**

Request

```
GET /wp-admin/includes/ HTTP/1.1
Cookie: wordpress_test_cookie=WP+Cookie+check
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0 Safari/537.36
Host: 10.255.112.211
Connection: Keep-alive
```

Recommendation

Restrict access to these directories or remove them from the website.

References

Web Server Security and Database Server Security
https://www.acunetix.com/websitesecurity/webserver-security/

WordPress REST API User Enumeration

WordPress includes a REST API that can be used to list the information about the registered users on a WordPress installation. The REST API exposed user data for all users who had authored a post of a public post type. WordPress 4.7.1 limits this to only post types which have specified that they should be shown within the REST API.

CWE
CWE-200

CVSS2
AV:N/AC:L/Au:N/C:N/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	None
Integrity Impact	None
Availability Impact	None

CVSS3
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	None
Integrity Impact	None
Availability Impact	None

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	None
Confidentiality Impact to the Vulnerable System	None
Integrity Impact to the Vulnerable System	None
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

An unauthenticated attacker can gain access to the list of users on a WordPress installation. This can be exploited by bots that are launching brute-force password guessing attacks on WordPress websites.

http://10.255.112.211/

Request

```
GET /?rest_route=/wp/v2/users HTTP/1.1
Cookie: wordpress_test_cookie=WP+Cookie+check
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0 Safari/537.36
Host: 10.255.112.211
Connection: Keep-alive
```

Recommendation

Install a WordPress plugin such as Stop User Enumeration. Stop User Enumeration is a security plugin designed to detect and prevent hackers scanning your site for user names.

References

Stop User Enumeration
https://wordpress.org/plugins/stop-user-enumeration/

WordPress 4.7.1 Security and Maintenance Release
https://wordpress.org/news/2017/01/wordpress-4-7-1-security-and-maintenance-release/

Error page web server version disclosure

Application errors or warning messages may disclose sensitive information about an application's internal workings to an attacker.

Acunetix found the web server version number and a list of modules enabled on the target server. Consult the 'Attack details' section for more information about the affected page.

CWE
CWE-200

CVSS2
AV:N/AC:L/Au:N/C:P/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	None
Availability Impact	None

CVSS3
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity Impact	None
Availability Impact	None

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N

Base Score	6.9
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	None
Confidentiality Impact to the Vulnerable System	Low
Integrity Impact to the Vulnerable System	None
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

Error messages information about an application's internal workings may be used to escalate attacks.

http://10.255.112.211/

Request

```
GET /zAMX80rZyh HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
```

```
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0 Safari/537.36
Host: 10.255.112.211
Connection: Keep-alive
```

Recommendation

Properly configure the web server not to disclose information about an application's internal workings to the user. Consult the 'Web references' section for more information.

References

Custom Error Responses (Apache HTTP Server)
https://httpd.apache.org/docs/current/custom-error.html

server_tokens (Nginx)
http://nginx.org/en/docs/http/ngx_http_core_module.html#server_tokens

Remove Unwanted HTTP Response Headers (Microsoft IIS)
https://blogs.msdn.microsoft.com/varunm/2013/04/23/remove-unwanted-http-response-headers/

Generic Email Address Disclosure

One or more email addresses have been found on this website. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.

CWE
CWE-200

CVSS2
AV:N/AC:L/Au:N/C:N/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	None
Integrity Impact	None
Availability Impact	None

CVSS3
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	None
Integrity Impact	None
Availability Impact	None

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	None
Confidentiality Impact to the Vulnerable System	None
Integrity Impact to the Vulnerable System	None
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

Email addresses posted on Web sites may attract spam.

http://10.255.112.211/

Emails found:

- http://10.255.112.211/license.txt
  m@tidakada.com

Request

```
GET /license.txt HTTP/1.1
Referer: http://10.255.112.211/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0 Safari/537.36
Host: 10.255.112.211
Connection: Keep-alive
```

Recommendation

Check references for details on how to solve this problem.

References

Anti-spam techniques
https://en.wikipedia.org/wiki/Anti-spam_techniques

Cookies with missing, inconsistent or contradictory properties

At least one of the following cookies properties causes the cookie to be invalid or incompatible with either a different property of the same cookie, of with the environment the cookie is being used in. Although this is not a vulnerability in itself, it will likely lead to unexpected behavior by the application, which in turn may cause secondary security issues.

CWE
CWE-284

CVSS2
AV:N/AC:L/Au:N/C:N/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	None
Integrity Impact	None
Availability Impact	None

CVSS3
CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	Required
Scope	Unchanged
Confidentiality	None
Integrity Impact	None
Availability Impact	None

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	Active
Confidentiality Impact to the Vulnerable System	None
Integrity Impact to the Vulnerable System	None
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

Cookies will not be stored, or submitted, by web browsers.

http://10.255.112.211/ Verified

List of cookies with missing, inconsistent or contradictory properties:

- http://10.255.112.211/wp-login.php

  Cookie was set with:

  ```
  Set-Cookie: wordpress_test_cookie=WP+Cookie+check; path=/
  ```

  This cookie has the following issues:

  ```
  - Cookie without SameSite attribute.
  When cookies lack the SameSite attribute, Web browsers may apply different and sometimes unexpected defaults. It is therefore
  recommended to add a SameSite attribute with an appropriate value of either "Strict", "Lax", or "None".
  ```

Request

```
GET /wp-login.php HTTP/1.1
Referer: http://10.255.112.211/readme.html
Cookie: wordpress_test_cookie=WP+Cookie+check
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0 Safari/537.36
```

```
Host: 10.255.112.211
Connection: Keep-alive
```

Recommendation

Ensure that the cookies configuration complies with the applicable standards.

References

MDN | Set-Cookie
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Set-Cookie

Securing cookies with cookie prefixes
https://www.sjoerdlangkemper.nl/2017/02/09/cookie-prefixes/

Cookies: HTTP State Management Mechanism
https://tools.ietf.org/html/draft-ietf-httpbis-rfc6265bis-05

SameSite Updates - The Chromium Projects
https://www.chromium.org/updates/same-site

draft-west-first-party-cookies-07: Same-site Cookies
https://tools.ietf.org/html/draft-west-first-party-cookies-07

WordPress Improper Authentication Vulnerability

Improper authentication vulnerability in WordPress versions prior to 6.0.3 allows a remote unauthenticated attacker to obtain the email address of the user who posted a blog using the WordPress Post by Email Feature. The developer also provides new patched releases for all versions since 3.7.

CWE
CWE-287

CVSS3
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity Impact	None
Availability Impact	None

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:P/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	Passive
Confidentiality Impact to the Vulnerable System	Low
Integrity Impact to the Vulnerable System	None
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

http://10.255.112.211/

wordpress v5.1.1-5.1.1

References

CVE-2022-43504
https://nvd.nist.gov/vuln/detail/CVE-2022-43504

WordPress Cross-Site Request Forgery (CSRF) Vulnerability

WordPress before 5.5.2 allows CSRF attacks that change a theme's background image.

CWE
CWE-352

CVSS3
CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N

Base Score	4.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	Required
Scope	Unchanged
Confidentiality	None
Integrity Impact	Low
Availability Impact	None

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N

Base Score	5.1
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	Active
Confidentiality Impact to the Vulnerable System	None
Integrity Impact to the Vulnerable System	Low
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

http://10.255.112.211/
wordpress v5.1.1-5.1.1

http://10.255.112.211/
wordpress v5.1.1-5.1.1

References

CVE-2020-28040
https://nvd.nist.gov/vuln/detail/CVE-2020-28040

Directory listings

Directory listing is a web server function that displays the directory contents when there is no index file in a specific website directory. It is dangerous to leave this function turned on for the web server because it leads to information disclosure.

CWE
CWE-538

CVSS2
AV:N/AC:L/Au:N/C:P/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	None
Availability Impact	None

CVSS3
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity Impact	None
Availability Impact	None

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N

Base Score	6.9
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	None
Confidentiality Impact to the Vulnerable System	Low
Integrity Impact to the Vulnerable System	None
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

A user can view a list of all files from the affected directories possibly exposing sensitive information.

http://10.255.112.211/ Verified

Folders with directory listing enabled:

- http://10.255.112.211/wp-admin/css/
- http://10.255.112.211/wp-admin/images/
- http://10.255.112.211/wp-includes/
- http://10.255.112.211/wp-includes/ID3/
- http://10.255.112.211/wp-includes/IXR/
- http://10.255.112.211/wp-includes/Requests/
- http://10.255.112.211/wp-includes/SimplePie/
- http://10.255.112.211/wp-admin/includes/
- http://10.255.112.211/wp-includes/Text/
- http://10.255.112.211/wp-admin/js/
- http://10.255.112.211/wp-includes/blocks/

Request

```
GET /wp-admin/css/ HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0 Safari/537.36
Host: 10.255.112.211
Connection: Keep-alive
```

Recommendation

You should make sure no sensitive information is disclosed or you may want to restrict directory listings from the web server configuration.

References

CWE-548: Exposure of Information Through Directory Listing
https://cwe.mitre.org/data/definitions/548.html

Documentation files

One or more documentation files (e.g. readme.txt, changelog.txt, ...) were found. The information contained in these files could help an attacker identify the web application you are using and sometimes the version of the application. It's recommended to remove these files from production systems.

CWE
CWE-538

CVSS2
AV:N/AC:L/Au:N/C:P/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	None
Availability Impact	None

CVSS3
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity Impact	None
Availability Impact	None

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N

Base Score	6.9
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	None
Confidentiality Impact to the Vulnerable System	Low
Integrity Impact to the Vulnerable System	None
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

These files may disclose sensitive information. This information can be used to launch further attacks.

http://10.255.112.211/

Documentation files:

- http://10.255.112.211/**readme.html**
  File contents (first 100 characters):

```
<!DOCTYPE html>
<html lang="en">
<head>
<meta name="viewport" content="width=device-width" />
<met ...
```

- http://10.255.112.211/**license.txt**
  File contents (first 100 characters):

```
WordPress - Web publishing software

Copyright 2011-2019 by the contributors

This program is fr ...
```

- http://10.255.112.211/wp-includes/ID3/**readme.txt**
  File contents (first 100 characters):

```
/////////////////////////////////////////////////////////////////
/// getID3() by James Heinrich <in ...
```

- http://10.255.112.211/wp-includes/ID3/**license.txt**
  File contents (first 100 characters):

```
/////////////////////////////////////////////////////////////////
/// getID3() by James Heinrich <in ...
```

Request

```
GET /readme.html HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0 Safari/537.36
Host: 10.255.112.211
Connection: Keep-alive
```

Recommendation

Remove or restrict access to all documentation file acessible from internet.

WordPress URL Redirection to Untrusted Site ('Open Redirect') Vulnerability

In affected versions of WordPress, due to an issue in wp_validate_redirect() and URL sanitization, an arbitrary external link can be crafted leading to unintended/open redirect when clicked. This has been patched in version 5.4.2, along with all the previously affected versions via a minor release (5.3.4, 5.2.7, 5.1.6, 5.0.10, 4.9.15, 4.8.14, 4.7.18, 4.6.19, 4.5.22, 4.4.23, 4.3.24, 4.2.28, 4.1.31, 4.0.31, 3.9.32, 3.8.34, 3.7.34).

CWE
CWE-601

CVSS3
CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:H/A:N

Base Score	5.7
Attack Vector	Network
Attack Complexity	Low
Privileges Required	Low
User Interaction	Required
Scope	Unchanged
Confidentiality	None
Integrity Impact	High

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:A/VC:N/VI:H/VA:N/SC:N/SI:N/SA:N

Base Score	6.8
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	Low
User Interaction	Active
Confidentiality Impact to the Vulnerable System	None
Integrity Impact to the Vulnerable System	High

Availability Impact	None

Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

http://10.255.112.211/

wordpress v5.1.1-5.1.1

http://10.255.112.211/

wordpress v5.1.1-5.1.1

References

CVE-2020-4048
https://nvd.nist.gov/vuln/detail/CVE-2020-4048

A02 Cryptographic Failures

The first thing is to determine the protection needs of data in transit and at rest. For example, passwords, credit card numbers, health records, personal information, and business secrets require extra protection, mainly if that data falls under privacy laws, e.g., EU's General Data Protection Regulation (GDPR), or regulations, e.g., financial data protection such as PCI Data Security Standard (PCI DSS).

Directory listings

Directory listing is a web server function that displays the directory contents when there is no index file in a specific website directory. It is dangerous to leave this function turned on for the web server because it leads to information disclosure.

CWE
CWE-538

CVSS2
AV:N/AC:L/Au:N/C:P/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	None
Availability Impact	None

CVSS3
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity Impact	None
Availability Impact	None

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N

Base Score	6.9
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	None
Confidentiality Impact to the Vulnerable System	Low
Integrity Impact to the Vulnerable System	None
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

A user can view a list of all files from the affected directories possibly exposing sensitive information.

http://10.255.112.211/ Verified

Folders with directory listing enabled:

- http://10.255.112.211/wp-admin/css/

- http://10.255.112.211/wp-admin/images/
- http://10.255.112.211/wp-includes/
- http://10.255.112.211/wp-includes/ID3/
- http://10.255.112.211/wp-includes/IXR/
- http://10.255.112.211/wp-includes/Requests/
- http://10.255.112.211/wp-includes/SimplePie/
- http://10.255.112.211/wp-admin/includes/
- http://10.255.112.211/wp-includes/Text/
- http://10.255.112.211/wp-admin/js/
- http://10.255.112.211/wp-includes/blocks/

Request

```
GET /wp-admin/css/ HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0 Safari/537.36
Host: 10.255.112.211
Connection: Keep-alive
```

Recommendation

You should make sure no sensitive information is disclosed or you may want to restrict directory listings from the web server configuration.

References

CWE-548: Exposure of Information Through Directory Listing
https://cwe.mitre.org/data/definitions/548.html

WordPress username enumeration

If permalinks are enabled, in many WordPress installations it is possible to enumerate all the WordPress usernames iterating through the author archives. Whenever a post is published, the username or alias is shown as the author. For example, the URL http://site.com/?author=1 will show all the posts from user id 1. Attackers can abuse this functionality to figure out which usernames are available on the site.

CWE

CWE-200

CVSS2

AV:N/AC:L/Au:N/C:P/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	None
Availability Impact	None

CVSS3

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity Impact	None
Availability Impact	None

CVSS4

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:P/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	Passive
Confidentiality Impact to the Vulnerable System	Low
Integrity Impact to the Vulnerable System	None
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

An attacker can enumerate the WordPress usernames and use this information to conduct brute-force attacks against passwords for these known usernames.

http://10.255.112.211/

List of WordPress users for {'_nativeUrl': {'password': '', 'username': '', 'search': '', 'protocol': 'http', 'port': '', 'path': '/', 'origin': 'http://10.255.112.211', 'href': 'http://10.255.112.211/', 'hostname': '10.255.112.211', 'host': '10.255.112.211', 'hash': ''}}:

['admin']

Request

```
POST //wp-login.php HTTP/1.1
Content-type: application/x-www-form-urlencoded
Cookie: wordpress_test_cookie=WP+Cookie+check
Content-Length: 28
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0 Safari/537.36
Host: 10.255.112.211
Connection: Keep-alive

log=10&pwd=z&wp-submit=Login
```

Recommendation

You can use an .htaccess rewrite rule to prevent this disclosure but you should also be sure to use nicknames to avoid disclosing usernames.

```
# Stop WordPress username enumeration vulnerability
RewriteCond %{REQUEST_URI} ^/$
RewriteCond %{QUERY_STRING} ^/?author=([0-9]*)
RewriteRule ^(.*)$ http://yoursite.com/somepage/? [L,R=301]
```

Documentation files

One or more documentation files (e.g. readme.txt, changelog.txt, ...) were found. The information contained in these files could help an attacker identify the web application you are using and sometimes the version of the application. It's recommended to remove these files from production systems.

CWE
CWE-538

CVSS2
AV:N/AC:L/Au:N/C:P/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	None
Availability Impact	None

CVSS3
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity Impact	None
Availability Impact	None

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N

Base Score	6.9
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	None
Confidentiality Impact to the Vulnerable System	Low
Integrity Impact to the Vulnerable System	None
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

These files may disclose sensitive information. This information can be used to launch further attacks.

http://10.255.112.211/

Documentation files:

- http://10.255.112.211/**readme.html**
  File contents (first 100 characters):

  ```
  <!DOCTYPE html>
  <html lang="en">
  <head>
  <meta name="viewport" content="width=device-width" />
  <met ...
  ```

- http://10.255.112.211/**license.txt**
  File contents (first 100 characters):

```
WordPress - Web publishing software

Copyright 2011-2019 by the contributors

This program is fr ...
```

- http://10.255.112.211/wp-includes/ID3/**readme.txt**
  File contents (first 100 characters):

```
/////////////////////////////////////////////////////////////////
/// getID3() by James Heinrich <in ...
```

- http://10.255.112.211/wp-includes/ID3/**license.txt**
  File contents (first 100 characters):

```
/////////////////////////////////////////////////////////////////
/// getID3() by James Heinrich <in ...
```

Request

```
GET /readme.html HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0 Safari/537.36
Host: 10.255.112.211
Connection: Keep-alive
```

Recommendation

Remove or restrict access to all documentation file acessible from internet.

Possible sensitive directories

One or more possibly sensitive directories were found. These resources are not directly linked from the website. This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.

CWE
CWE-200

CVSS2
AV:N/AC:L/Au:N/C:P/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	None
Availability Impact	None

CVSS3
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity Impact	None
Availability Impact	None

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N

Base Score	6.9
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	None
Confidentiality Impact to the Vulnerable System	Low
Integrity Impact to the Vulnerable System	None
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

These directories may expose sensitive information that could help a malicious user to prepare more advanced attacks.

http://10.255.112.211/

Possible sensitive directories:

- http://10.255.112.211/wp-admin/**includes**

Request

```
GET /wp-admin/includes/ HTTP/1.1
Cookie: wordpress_test_cookie=WP+Cookie+check
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0 Safari/537.36
Host: 10.255.112.211
Connection: Keep-alive
```

Recommendation

Restrict access to these directories or remove them from the website.

References

Web Server Security and Database Server Security
https://www.acunetix.com/websitesecurity/webserver-security/

WordPress REST API User Enumeration

WordPress includes a REST API that can be used to list the information about the registered users on a WordPress installation. The REST API exposed user data for all users who had authored a post of a public post type. WordPress 4.7.1 limits this to only post types which have specified that they should be shown within the REST API.

CWE
CWE-200

CVSS2
AV:N/AC:L/Au:N/C:N/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	None
Integrity Impact	None
Availability Impact	None

CVSS3
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	None
Integrity Impact	None
Availability Impact	None

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	None
Confidentiality Impact to the Vulnerable System	None
Integrity Impact to the Vulnerable System	None
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

An unauthenticated attacker can gain access to the list of users on a WordPress installation. This can be exploited by bots that are launching brute-force password guessing attacks on WordPress websites.

http://10.255.112.211/

Request

```
GET /?rest_route=/wp/v2/users HTTP/1.1
Cookie: wordpress_test_cookie=WP+Cookie+check
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0 Safari/537.36
Host: 10.255.112.211
Connection: Keep-alive
```

Recommendation

Install a WordPress plugin such as Stop User Enumeration. Stop User Enumeration is a security plugin designed to detect and prevent hackers scanning your site for user names.

References

Stop User Enumeration
https://wordpress.org/plugins/stop-user-enumeration/

WordPress 4.7.1 Security and Maintenance Release
https://wordpress.org/news/2017/01/wordpress-4-7-1-security-and-maintenance-release/

Error page web server version disclosure

Application errors or warning messages may disclose sensitive information about an application's internal workings to an attacker.

Acunetix found the web server version number and a list of modules enabled on the target server. Consult the 'Attack details' section for more information about the affected page.

CWE
CWE-200

CVSS2
AV:N/AC:L/Au:N/C:P/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	None
Availability Impact	None

CVSS3
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity Impact	None
Availability Impact	None

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N

Base Score	6.9
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	None
Confidentiality Impact to the Vulnerable System	Low
Integrity Impact to the Vulnerable System	None
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

Error messages information about an application's internal workings may be used to escalate attacks.

http://10.255.112.211/

Request

```
GET /zAMX80rZyh HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0 Safari/537.36
Host: 10.255.112.211
Connection: Keep-alive
```

Recommendation

Properly configure the web server not to disclose information about an application's internal workings to the user. Consult the 'Web references' section for more information.

References

Custom Error Responses (Apache HTTP Server)
https://httpd.apache.org/docs/current/custom-error.html

server_tokens (Nginx)
http://nginx.org/en/docs/http/ngx_http_core_module.html#server_tokens

Remove Unwanted HTTP Response Headers (Microsoft IIS)
https://blogs.msdn.microsoft.com/varunm/2013/04/23/remove-unwanted-http-response-headers/

Generic Email Address Disclosure

One or more email addresses have been found on this website. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.

CWE
CWE-200

CVSS2
AV:N/AC:L/Au:N/C:N/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	None
Integrity Impact	None
Availability Impact	None

CVSS3
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	None
Integrity Impact	None
Availability Impact	None

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	None
Confidentiality Impact to the Vulnerable System	None
Integrity Impact to the Vulnerable System	None
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

Email addresses posted on Web sites may attract spam.

http://10.255.112.211/

Emails found:

- http://10.255.112.211/license.txt
  m@tidakada.com

Request

```
GET /license.txt HTTP/1.1
Referer: http://10.255.112.211/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0 Safari/537.36
Host: 10.255.112.211
Connection: Keep-alive
```

Recommendation

Check references for details on how to solve this problem.

References

Anti-spam techniques
https://en.wikipedia.org/wiki/Anti-spam_techniques

SSL/TLS Not Implemented

This scan target was connected to over an unencrypted connection. A potential attacker can intercept and modify data sent and received from this site.

CWE
CWE-319

CVSS2

AV:N/AC:M/Au:N/C:P/I:P/A:N

Access Vector	Network
Access Complexity	Medium
Authentication	None
Confidentiality	Partial
Integrity Impact	Partial
Availability Impact	None

CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N

Base Score	5.4
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	Required
Scope	Unchanged
Confidentiality	Low
Integrity Impact	Low
Availability Impact	None

CVSS4

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N

Base Score	5.1
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	Active
Confidentiality Impact to the Vulnerable System	Low
Integrity Impact to the Vulnerable System	Low
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

Possible information disclosure.

http://10.255.112.211/ Verified

Request

```
GET / HTTP/1.1
Referer: http://10.255.112.211/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0 Safari/537.36
Host: 10.255.112.211
Connection: Keep-alive
```

Recommendation

The site should send and receive data over a secure (HTTPS) connection.

A03 Injection

Injection flaws, such as SQL, NoSQL, OS, and LDAP injection, occur when untrusted data is sent an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.

WordPress Improper Input Validation Vulnerability

wp_kses_bad_protocol in wp-includes/kses.php in WordPress before 5.3.1 mishandles the HTML5 colon named entity, allowing attackers to bypass input sanitization, as demonstrated by the javascript: substring.

CWE

CWE-20

CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Base Score	9.8
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	High

CVSS4

CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N

Base Score	8.7
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	Low
User Interaction	None
Confidentiality Impact to the Vulnerable System	High

Integrity Impact	High
Availability Impact	High

Integrity Impact to the Vulnerable System	High
Availability Impact to the Vulnerable System	High
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

http://10.255.112.211/

wordpress v5.1.1-5.1.1

http://10.255.112.211/

wordpress v5.1.1-5.1.1

http://10.255.112.211/

wordpress v5.1.1-5.1.1

References

CVE-2019-20041
https://nvd.nist.gov/vuln/detail/CVE-2019-20041

WordPress 5.1.x Multiple Vulnerabilities

WordPress is prone to multiple vulnerabilities, including cross-site scripting and SQL injection vulnerabilities. Exploiting these issues could allow an attacker to execute arbitrary script code in the browser of an unsuspecting user in the context of the affected site, allowing the attacker to steal cookie-based authentication credentials, or to compromise the application, access or modify data or exploit vulnerabilities in the underlying database. WordPress versions 5.1.x ranging from 5.1 and up to (and including) 5.1.13 are vulnerable.

CWE
CWE-89

CVSS2
AV:N/AC:H/Au:S/C:P/I:P/A:P/E:H/RL:OF/RC:C

Access Vector	Network
Access Complexity	High
Authentication	Single
Confidentiality	Partial
Integrity Impact	Partial
Availability Impact	Partial
Exploitability	High
Remediation Level	Official Fix
Report Confidence	Confirmed

CVSS3
CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H

Base Score	8
Attack Vector	Network
Attack Complexity	High
Privileges Required	High
User Interaction	None
Scope	Changed
Confidentiality	High
Integrity Impact	High
Availability Impact	High

CVSS4
CVSS:4.0/AV:N/AC:H/AT:N/PR:H/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N

Base Score	7.5
Attack Vector	Network
Attack Complexity	High
Attack Requirements	None
Privileges Required	High
User Interaction	None
Confidentiality Impact to the Vulnerable System	High
Integrity Impact to the Vulnerable System	High
Availability Impact to the Vulnerable System	High
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

http://10.255.112.211/

wordpress v5.1.1-5.1.1

http://10.255.112.211/

wordpress v5.1.1-5.1.1

http://10.255.112.211/

wordpress v5.1.1-5.1.1

http://10.255.112.211/

wordpress v5.1.1-5.1.1

http://10.255.112.211/

wordpress v5.1.1-5.1.1

http://10.255.112.211/

wordpress v5.1.1-5.1.1

http://10.255.112.211/

wordpress v5.1.1-5.1.1

http://10.255.112.211/

wordpress v5.1.1-5.1.1

http://10.255.112.211/

wordpress v5.1.1-5.1.1

http://10.255.112.211/

wordpress v5.1.1-5.1.1

http://10.255.112.211/

wordpress v5.1.1-5.1.1

Recommendation

Update to WordPress version 5.1.14 or latest

References

https://www.wordfence.com/blog/2022/08/wordpress-core-6-0-2-security-maintenance-release-what-you-need-to-know/
https://www.wordfence.com/blog/2022/08/wordpress-core-6-0-2-security-maintenance-release-what-you-need-to-know/

https://wordpress.org/news/2022/08/wordpress-6-0-2-security-and-maintenance-release/
https://wordpress.org/news/2022/08/wordpress-6-0-2-security-and-maintenance-release/

WordPress Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') Vulnerability

WordPress is a free and open-source content management system written in PHP and paired with a MariaDB database. Due to lack of proper sanitization in one of the classes, there's potential for unintended SQL queries to be executed. This has been patched in WordPress version 5.8.3. Older affected versions are also fixed via security release, that go back till 4.1.34. We strongly recommend that you keep auto-updates enabled. There are no known workarounds for this issue.

CWE
CWE-138

CVSS3
CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Base Score	8.8
Attack Vector	Network
Attack Complexity	Low
Privileges Required	Low
User Interaction	None

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N

Base Score	9.3
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None

Scope	Unchanged
Confidentiality	High
Integrity Impact	High
Availability Impact	High

User Interaction	None
Confidentiality Impact to the Vulnerable System	High
Integrity Impact to the Vulnerable System	High
Availability Impact to the Vulnerable System	High
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

http://10.255.112.211/

wordpress v5.1.1-5.1.1

http://10.255.112.211/

wordpress v5.1.1-5.1.1

http://10.255.112.211/

wordpress v5.1.1-5.1.1

http://10.255.112.211/

wordpress v5.1.1-5.1.1

http://10.255.112.211/

wordpress v5.1.1-5.1.1

References

CVE-2022-21664
https://nvd.nist.gov/vuln/detail/CVE-2022-21664

A04 Insecure Design

Insecure design is a broad category representing different weaknesses, expressed as "missing or ineffective control design." Insecure design is not the source for all other Top 10 risk categories. There is a difference between insecure design and insecure implementation. We differentiate between design flaws and implementation defects for a reason, they have different root causes and remediation. A secure design can still have implementation defects leading to vulnerabilities that may be exploited. An insecure design cannot be fixed by a perfect implementation as by definition, needed security controls were never created to defend against specific attacks. One of the factors that contribute to insecure design is the lack of business risk profiling inherent in the software or system being developed, and thus the failure to determine what level of security design is required.

WordPress Improper Privilege Management Vulnerability

WordPress before 5.5.2 allows attackers to gain privileges via XML-RPC.

CWE
CWE-269

CVSS3
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Base Score	9.8
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	High

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N

Base Score	8.7
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	Low
User Interaction	None
Confidentiality Impact to the Vulnerable System	High

Integrity Impact	High
Availability Impact	High

Integrity Impact to the Vulnerable System	High
Availability Impact to the Vulnerable System	High
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

http://10.255.112.211/

wordpress v5.1.1-5.1.1

http://10.255.112.211/

wordpress v5.1.1-5.1.1

http://10.255.112.211/

wordpress v5.1.1-5.1.1

References

CVE-2020-28035
https://nvd.nist.gov/vuln/detail/CVE-2020-28035

WordPress 5.1.x Multiple Vulnerabilities

WordPress is prone to multiple vulnerabilities, including cross-site scripting, privilege escalation, security bypass, Denial of Service and PHP object injection vulnerabilities. Exploiting these issues could allow an attacker to execute arbitrary script code in the browser of an unsuspecting user in the context of the affected site, allowing the attacker to steal cookie-based authentication credentials and launch other attacks, to bypass the expected capabilities check, to perform otherwise restricted actions and subsequently delete arbitrary files, to deny service to legitimate users, or to possibly execute arbitrary PHP code within the context of the affected webserver process. WordPress versions 5.1.x ranging from 5.1 and up to (and including) 5.1.6 are vulnerable.

CWE

CWE-502

CVSS2

AV:N/AC:M/Au:S/C:P/I:P/A:P/E:H/RL:OF/RC:C

Access Vector	Network
Access Complexity	Medium
Authentication	Single
Confidentiality	Partial
Integrity Impact	Partial
Availability Impact	Partial
Exploitability	High
Remediation Level	Official Fix
Report Confidence	Confirmed

CVSS3

CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:L

Base Score	6.5
Attack Vector	Network
Attack Complexity	Low
Privileges Required	Low
User Interaction	Required
Scope	Changed
Confidentiality	Low
Integrity Impact	Low
Availability Impact	Low

CVSS4

CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:A/VC:L/VI:L/VA:L/SC:N/SI:N/SA

Base Score	4.8
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	Low
User Interaction	Active
Confidentiality Impact to the Vulnerable System	Low
Integrity Impact to the Vulnerable System	Low
Availability Impact to the Vulnerable System	Low
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

http://10.255.112.211/

wordpress v5.1.1-5.1.1

http://10.255.112.211/

wordpress v5.1.1-5.1.1

Recommendation

Update to WordPress version 5.1.7 or latest

References

https://blog.sucuri.net/2020/10/reflected-xss-in-wordpress-v5-5-1-and-lower.html
https://blog.sucuri.net/2020/10/reflected-xss-in-wordpress-v5-5-1-and-lower.html

https://blog.wpscan.com/2020/10/30/wordpress-5.5.2-security-release.html
https://blog.wpscan.com/2020/10/30/wordpress-5.5.2-security-release.html

https://threatpost.com/wordpress-patches-rce-bug/160812/
https://threatpost.com/wordpress-patches-rce-bug/160812/

https://wordpress.org/support/wordpress-version/version-5-1-7/
https://wordpress.org/support/wordpress-version/version-5-1-7/

Content Security Policy (CSP) Not Implemented

Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks.

Content Security Policy (CSP) can be implemented by adding a **Content-Security-Policy** header. The value of this header is a string containing the policy directives describing your Content Security Policy. To implement CSP, you should define lists of allowed origins for the all of the types of resources that your site utilizes. For example, if you have a simple site that needs to load scripts, stylesheets, and images hosted locally, as well as from the jQuery library from their CDN, the CSP header could look like the following:

```
Content-Security-Policy:
default-src 'self';
script-src 'self' https://code.jquery.com;
```

It was detected that your web application doesn't implement Content Security Policy (CSP) as the CSP header is missing from the response. It's recommended to implement Content Security Policy (CSP) into your web application.

CWE
CWE-1021

CVSS2
AV:N/AC:L/Au:N/C:N/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	None
Integrity Impact	None
Availability Impact	None

CVSS3
CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:N/A:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	Required
Scope	Changed
Confidentiality	None
Integrity Impact	None
Availability Impact	None

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	Active
Confidentiality Impact to the Vulnerable System	None
Integrity Impact to the Vulnerable System	None
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

CSP can be used to prevent and/or mitigate attacks that involve content/code injection, such as cross-site scripting/XSS attacks, attacks that require embedding a malicious resource, attacks that involve malicious use of iframes, such as clickjacking attacks, and others.

http://10.255.112.211/

Paths without CSP header:

- http://10.255.112.211/readme.html

- http://10.255.112.211/wp-admin/images/
- http://10.255.112.211/wp-login.php
- http://10.255.112.211/index.php
- http://10.255.112.211/wp-admin/install.php
- http://10.255.112.211/wp-admin/upgrade.php
- http://10.255.112.211/wp-admin/css/
- http://10.255.112.211/wp-content/
- http://10.255.112.211/wp-includes/
- http://10.255.112.211/wp-includes/ID3/
- http://10.255.112.211/wp-includes/ID3/getid3.lib.php
- http://10.255.112.211/wp-content/plugins/
- http://10.255.112.211/wp-content/themes/
- http://10.255.112.211/wp-includes/IXR/
- http://10.255.112.211/wp-includes/IXR/class-IXR-base64.php
- http://10.255.112.211/wp-includes/Requests/
- http://10.255.112.211/wp-includes/SimplePie/
- http://10.255.112.211/wp-includes/Text/
- http://10.255.112.211/wp-admin/includes/
- http://10.255.112.211/wp-includes/Text/Diff.php
- http://10.255.112.211/wp-admin/js/

Request

```
GET /readme.html HTTP/1.1
Referer: http://10.255.112.211/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0 Safari/537.36
Host: 10.255.112.211
Connection: Keep-alive
```

Recommendation

It's recommended to implement Content Security Policy (CSP) into your web application. Configuring Content Security Policy involves adding the **Content-Security-Policy** HTTP header to a web page and giving it values to control resources the user agent is allowed to load for that page.

References

Content Security Policy (CSP)
https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP

Implementing Content Security Policy
https://hacks.mozilla.org/2016/02/implementing-content-security-policy/

Permissions-Policy header not implemented

The Permissions-Policy header allows developers to selectively enable and disable use of various browser features and APIs.

CWE
CWE-1021

CVSS2
AV:N/AC:L/Au:N/C:N/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	None
Integrity Impact	None
Availability Impact	None

CVSS3
CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:N/A:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	Required
Scope	Changed
Confidentiality	None
Integrity Impact	None
Availability Impact	None

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	Active
Confidentiality Impact to the Vulnerable System	None
Integrity Impact to the Vulnerable System	None
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

http://10.255.112.211/

Locations without Permissions-Policy header:

- http://10.255.112.211/readme.html
- http://10.255.112.211/wp-admin/images/
- http://10.255.112.211/wp-login.php
- http://10.255.112.211/icons/
- http://10.255.112.211/index.php
- http://10.255.112.211/wp-admin/install.php
- http://10.255.112.211/wp-admin/upgrade.php
- http://10.255.112.211/wp-admin/css/
- http://10.255.112.211/wp-content/
- http://10.255.112.211/wp-includes/
- http://10.255.112.211/wp-includes/ID3/
- http://10.255.112.211/wp-includes/ID3/getid3.lib.php
- http://10.255.112.211/wp-content/plugins/
- http://10.255.112.211/wp-content/themes/
- http://10.255.112.211/wp-includes/IXR/
- http://10.255.112.211/wp-includes/IXR/class-IXR-base64.php
- http://10.255.112.211/wp-includes/Requests/
- http://10.255.112.211/wp-includes/SimplePie/
- http://10.255.112.211/wp-includes/Text/
- http://10.255.112.211/wp-admin/includes/
- http://10.255.112.211/wp-includes/Text/Diff.php

Request

```
GET /readme.html HTTP/1.1
Referer: http://10.255.112.211/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0 Safari/537.36
Host: 10.255.112.211
Connection: Keep-alive
```

References

Permissions-Policy / Feature-Policy (MDN)
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Feature-Policy

Permissions Policy (W3C)
https://www.w3.org/TR/permissions-policy-1/

A05 Security Misconfiguration

Security misconfiguration is commonly a result of insecure default configurations, incomplete or ad hoc configurations, open cloud storage, misconfigured HTTP headers, and verbose error messages containing sensitive information. Not only must all operating systems, frameworks, libraries, and applications be securly configured, but they must be patched and upgraded in a timely fashion.

Directory listings

Directory listing is a web server function that displays the directory contents when there is no index file in a specific website directory. It is dangerous to leave this function turned on for the web server because it leads to information disclosure.

CWE
CWE-538

CVSS2
AV:N/AC:L/Au:N/C:P/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	None
Availability Impact	None

CVSS3
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity Impact	None
Availability Impact	None

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N

Base Score	6.9
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	None
Confidentiality Impact to the Vulnerable System	Low
Integrity Impact to the Vulnerable System	None
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

A user can view a list of all files from the affected directories possibly exposing sensitive information.

http://10.255.112.211/ Verified

Folders with directory listing enabled:

- http://10.255.112.211/wp-admin/css/
- http://10.255.112.211/wp-admin/images/
- http://10.255.112.211/wp-includes/
- http://10.255.112.211/wp-includes/ID3/
- http://10.255.112.211/wp-includes/IXR/
- http://10.255.112.211/wp-includes/Requests/
- http://10.255.112.211/wp-includes/SimplePie/
- http://10.255.112.211/wp-admin/includes/
- http://10.255.112.211/wp-includes/Text/
- http://10.255.112.211/wp-admin/js/
- http://10.255.112.211/wp-includes/blocks/

Request

```
GET /wp-admin/css/ HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0 Safari/537.36
Host: 10.255.112.211
Connection: Keep-alive
```

Recommendation

You should make sure no sensitive information is disclosed or you may want to restrict directory listings from the web server configuration.

References

CWE-548: Exposure of Information Through Directory Listing
https://cwe.mitre.org/data/definitions/548.html

Cookies Not Marked as HttpOnly

One or more cookies don't have the HttpOnly flag set. When a cookie is set with the HttpOnly flag, it instructs the browser that the cookie can only be accessed by the server and not by client-side scripts. This is an important security protection for session cookies.

CWE
CWE-1004

CVSS2
AV:N/AC:L/Au:N/C:N/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	None
Integrity Impact	None
Availability Impact	None

CVSS3
CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	Required
Scope	Unchanged
Confidentiality	None
Integrity Impact	None
Availability Impact	None

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	Active
Confidentiality Impact to the Vulnerable System	None
Integrity Impact to the Vulnerable System	None
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

Cookies can be accessed by client-side scripts.

http://10.255.112.211/ Verified

Cookies without HttpOnly flag set:

- http://10.255.112.211/wp-login.php

```
Set-Cookie: wordpress_test_cookie=WP+Cookie+check; path=/
```

Request

```
GET /wp-login.php HTTP/1.1
Referer: http://10.255.112.211/readme.html
Cookie: wordpress_test_cookie=WP+Cookie+check
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0 Safari/537.36
Host: 10.255.112.211
Connection: Keep-alive
```

Recommendation

If possible, you should set the HttpOnly flag for these cookies.

Cookies with missing, inconsistent or contradictory properties

At least one of the following cookies properties causes the cookie to be invalid or incompatible with either a different property of the same cookie, of with the environment the cookie is being used in. Although this is not a vulnerability in itself, it will likely lead to unexpected behavior by the application, which in turn may cause secondary security issues.

CWE
CWE-284

CVSS2
AV:N/AC:L/Au:N/C:N/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	None
Integrity Impact	None
Availability Impact	None

CVSS3
CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	Required
Scope	Unchanged
Confidentiality	None
Integrity Impact	None
Availability Impact	None

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	Active
Confidentiality Impact to the Vulnerable System	None
Integrity Impact to the Vulnerable System	None
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

Cookies will not be stored, or submitted, by web browsers.

http://10.255.112.211/ Verified

List of cookies with missing, inconsistent or contradictory properties:

- http://10.255.112.211/wp-login.php

  Cookie was set with:

  ```
  Set-Cookie: wordpress_test_cookie=WP+Cookie+check; path=/
  ```

  This cookie has the following issues:

  ```
  - Cookie without SameSite attribute.
  When cookies lack the SameSite attribute, Web browsers may apply different and sometimes unexpected defaults. It is therefore
  recommended to add a SameSite attribute with an appropriate value of either "Strict", "Lax", or "None".
  ```

Request

```
GET /wp-login.php HTTP/1.1
Referer: http://10.255.112.211/readme.html
Cookie: wordpress_test_cookie=WP+Cookie+check
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0 Safari/537.36
Host: 10.255.112.211
Connection: Keep-alive
```

Recommendation

Ensure that the cookies configuration complies with the applicable standards.

References

MDN | Set-Cookie
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Set-Cookie

Securing cookies with cookie prefixes

https://www.sjoerdlangkemper.nl/2017/02/09/cookie-prefixes/
Cookies: HTTP State Management Mechanism
https://tools.ietf.org/html/draft-ietf-httpbis-rfc6265bis-05

SameSite Updates - The Chromium Projects
https://www.chromium.org/updates/same-site

draft-west-first-party-cookies-07: Same-site Cookies
https://tools.ietf.org/html/draft-west-first-party-cookies-07

WordPress admin accessible without HTTP authentication

It's recommended to restrict access to the WordPress administration dashboard using HTTP authentication. Password protecting your WordPress admin dashboard through a layer of HTTP authentication is an effective measure to thwart attackers attempting to guess user's passwords. Additionally, if attackers manage to steal a user's password, they will need to get past HTTP authentication in order to gain access to WordPress login form.

CWE
CWE-16

CVSS2
AV:N/AC:L/Au:N/C:N/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	None
Integrity Impact	None
Availability Impact	None

CVSS3
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	None
Integrity Impact	None
Availability Impact	None

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	None
Confidentiality Impact to the Vulnerable System	None
Integrity Impact to the Vulnerable System	None
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

No impact is associated with this vulnerability.

http://10.255.112.211/wp-admin/

Request

```
GET /wp-admin/ HTTP/1.1
Cookie: wordpress_test_cookie=WP+Cookie+check
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0 Safari/537.36
Host: 10.255.112.211
Connection: Keep-alive
```

Recommendation

Add server-side password protection (such as BasicAuth) to the /wp-admin/ directory. Consult web references for more information.

References

Securing wp-admin
https://codex.wordpress.org/Hardening_WordPress

WordPress Security Tips Part 5 | Restrict Access to wp-admin Directory
https://www.acunetix.com/blog/articles/wordpress-security-wpadmin-directory/

WordPress default administrator account

By default WordPress creates an administrator user account named **admin**. Using the default Admin WordPress Account, hackers can easily launch a brute force attack against it. In order to help deter this type of attack, you should change your default WordPress administrator username to something more difficult to guess.

CWE
CWE-16

CVSS2
AV:N/AC:L/Au:N/C:N/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	None
Integrity Impact	None
Availability Impact	None

CVSS3
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	None
Integrity Impact	None
Availability Impact	None

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	None
Confidentiality Impact to the Vulnerable System	None
Integrity Impact to the Vulnerable System	None
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

No impact is associated with this vulnerability.

http://10.255.112.211/wp-login.php

Request

```
POST //wp-login.php HTTP/1.1
Content-type: application/x-www-form-urlencoded
Cookie: wordpress_test_cookie=WP+Cookie+check
Content-Length: 41
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0 Safari/537.36
Host: 10.255.112.211
Connection: Keep-alive

log=admin&pwd=testingtest&wp-submit=Login
```

Recommendation

Change the default WordPress administrator username to something more difficult to guess. Consult web references for more information.

References

OWASP Wordpress Security Implementation Guideline
https://www.owasp.org/index.php/OWASP_Wordpress_Security_Implementation_Guideline#Remove_or_change_the_default_administrator_account

Your WordPress Installation Is Using the Default Admin Account
https://www.acunetix.com/blog/wordpress-security/wordpress-default-admin-account/

Change WordPress admin username for security
https://www.inmotionhosting.com/support/website/wordpress/change-wordpress-admin-username-for-security

Content Security Policy (CSP) Not Implemented

Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks.

Content Security Policy (CSP) can be implemented by adding a **Content-Security-Policy** header. The value of this header is a string containing the policy directives describing your Content Security Policy. To implement CSP, you should define lists of allowed origins for the all of the types of resources that your site utilizes. For example, if you have a simple site that needs to load scripts, stylesheets, and images hosted locally, as well as from the jQuery library from their CDN, the CSP header could look like the following:

```
Content-Security-Policy:
default-src 'self';
script-src 'self' https://code.jquery.com;
```

It was detected that your web application doesn't implement Content Security Policy (CSP) as the CSP header is missing from the response. It's recommended to implement Content Security Policy (CSP) into your web application.

CWE
CWE-1021

CVSS2
AV:N/AC:L/Au:N/C:N/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	None
Integrity Impact	None
Availability Impact	None

CVSS3
CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:N/A:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	Required
Scope	Changed
Confidentiality	None
Integrity Impact	None
Availability Impact	None

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	Active
Confidentiality Impact to the Vulnerable System	None
Integrity Impact to the Vulnerable System	None
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

CSP can be used to prevent and/or mitigate attacks that involve content/code injection, such as cross-site scripting/XSS attacks, attacks that require embedding a malicious resource, attacks that involve malicious use of iframes, such as clickjacking attacks, and others.

http://10.255.112.211/

Paths without CSP header:

- http://10.255.112.211/readme.html
- http://10.255.112.211/wp-admin/images/
- http://10.255.112.211/wp-login.php
- http://10.255.112.211/index.php
- http://10.255.112.211/wp-admin/install.php
- http://10.255.112.211/wp-admin/upgrade.php
- http://10.255.112.211/wp-admin/css/
- http://10.255.112.211/wp-content/
- http://10.255.112.211/wp-includes/
- http://10.255.112.211/wp-includes/ID3/
- http://10.255.112.211/wp-includes/ID3/getid3.lib.php
- http://10.255.112.211/wp-content/plugins/
- http://10.255.112.211/wp-content/themes/
- http://10.255.112.211/wp-includes/IXR/

- http://10.255.112.211/wp-includes/IXR/class-IXR-base64.php
- http://10.255.112.211/wp-includes/Requests/
- http://10.255.112.211/wp-includes/SimplePie/
- http://10.255.112.211/wp-includes/Text/
- http://10.255.112.211/wp-admin/includes/
- http://10.255.112.211/wp-includes/Text/Diff.php
- http://10.255.112.211/wp-admin/js/

Request

```
GET /readme.html HTTP/1.1
Referer: http://10.255.112.211/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0 Safari/537.36
Host: 10.255.112.211
Connection: Keep-alive
```

Recommendation

It's recommended to implement Content Security Policy (CSP) into your web application. Configuring Content Security Policy involves adding the **Content-Security-Policy** HTTP header to a web page and giving it values to control resources the user agent is allowed to load for that page.

References

Content Security Policy (CSP)
https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP

Implementing Content Security Policy
https://hacks.mozilla.org/2016/02/implementing-content-security-policy/

Error page web server version disclosure

Application errors or warning messages may disclose sensitive information about an application's internal workings to an attacker.

Acunetix found the web server version number and a list of modules enabled on the target server. Consult the 'Attack details' section for more information about the affected page.

CWE
CWE-200

CVSS2
AV:N/AC:L/Au:N/C:P/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	None
Availability Impact	None

CVSS3
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity Impact	None
Availability Impact	None

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N

Base Score	6.9
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	None
Confidentiality Impact to the Vulnerable System	Low
Integrity Impact to the Vulnerable System	None
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

Error messages information about an application's internal workings may be used to escalate attacks.

http://10.255.112.211/

Request

```
GET /zAMX80rZyh HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0 Safari/537.36
Host: 10.255.112.211
Connection: Keep-alive
```

Recommendation

Properly configure the web server not to disclose information about an application's internal workings to the user. Consult the 'Web references' section for more information.

References

Custom Error Responses (Apache HTTP Server)
https://httpd.apache.org/docs/current/custom-error.html

server_tokens (Nginx)
http://nginx.org/en/docs/http/ngx_http_core_module.html#server_tokens

Remove Unwanted HTTP Response Headers (Microsoft IIS)
https://blogs.msdn.microsoft.com/varunm/2013/04/23/remove-unwanted-http-response-headers/

Permissions-Policy header not implemented

The Permissions-Policy header allows developers to selectively enable and disable use of various browser features and APIs.

CWE
CWE-1021

CVSS2
AV:N/AC:L/Au:N/C:N/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	None
Integrity Impact	None
Availability Impact	None

CVSS3
CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:N/A:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	Required
Scope	Changed
Confidentiality	None
Integrity Impact	None
Availability Impact	None

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	Active
Confidentiality Impact to the Vulnerable System	None
Integrity Impact to the Vulnerable System	None
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

http://10.255.112.211/

Locations without Permissions-Policy header:

- http://10.255.112.211/readme.html
- http://10.255.112.211/wp-admin/images/
- http://10.255.112.211/wp-login.php
- http://10.255.112.211/icons/
- http://10.255.112.211/index.php
- http://10.255.112.211/wp-admin/install.php

- http://10.255.112.211/wp-admin/upgrade.php
- http://10.255.112.211/wp-admin/css/
- http://10.255.112.211/wp-content/
- http://10.255.112.211/wp-includes/
- http://10.255.112.211/wp-includes/ID3/
- http://10.255.112.211/wp-includes/ID3/getid3.lib.php
- http://10.255.112.211/wp-content/plugins/
- http://10.255.112.211/wp-content/themes/
- http://10.255.112.211/wp-includes/IXR/
- http://10.255.112.211/wp-includes/IXR/class-IXR-base64.php
- http://10.255.112.211/wp-includes/Requests/
- http://10.255.112.211/wp-includes/SimplePie/
- http://10.255.112.211/wp-includes/Text/
- http://10.255.112.211/wp-admin/includes/
- http://10.255.112.211/wp-includes/Text/Diff.php

Request

```
GET /readme.html HTTP/1.1
Referer: http://10.255.112.211/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0 Safari/537.36
Host: 10.255.112.211
Connection: Keep-alive
```

References

Permissions-Policy / Feature-Policy (MDN)
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Feature-Policy

Permissions Policy (W3C)
https://www.w3.org/TR/permissions-policy-1/

Subresource Integrity (SRI) Not Implemented

Subresource Integrity (SRI) is a security feature that enables browsers to verify that third-party resources they fetch (for example, from a CDN) are delivered without unexpected manipulation. It works by allowing developers to provide a cryptographic hash that a fetched file must match.

Third-party resources (such as scripts and stylesheets) can be manipulated. An attacker that has access or has hacked the hosting CDN can manipulate or replace the files. SRI allows developers to specify a base64-encoded cryptographic hash of the resource to be loaded. The integrity attribute containing the hash is then added to the <script> HTML element tag. The integrity string consists of a base64-encoded hash, followed by a prefix that depends on the hash algorithm. This prefix can either be sha256, sha384 or sha512.

The script loaded from the external URL specified in the Details section doesn't implement Subresource Integrity (SRI). It's recommended to implement Subresource Integrity (SRI) for all the scripts loaded from external hosts.

CWE
CWE-830

CVSS2
AV:N/AC:L/Au:N/C:N/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	None
Integrity Impact	None
Availability Impact	None

CVSS3
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Changed
Confidentiality	None
Integrity Impact	None
Availability Impact	None

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N

Base Score	6.9
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	None
Confidentiality Impact to the Vulnerable System	None
Integrity Impact to the Vulnerable System	Low
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

An attacker that has access or has hacked the hosting CDN can manipulate or replace the files.

http://10.255.112.211/index.php

Pages where SRI is not implemented:

- http://10.255.112.211/index.php
  Script SRC: **http://wordy/wp-includes/js/jquery/jquery.js?ver=1.12.4**

Request

```
GET /index.php HTTP/1.1
Referer: http://10.255.112.211/
Cookie: wordpress_test_cookie=WP+Cookie+check
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0 Safari/537.36
Host: 10.255.112.211
Connection: Keep-alive
```

Recommendation

Use the SRI Hash Generator link (from the References section) to generate a <script> element that implements Subresource Integrity (SRI).

For example, you can use the following <script> element to tell a browser that before executing the https://example.com/example-framework.js script, the browser must first compare the script to the expected hash, and verify that there's a match.

```
<script src="https://example.com/example-framework.js"
integrity="sha384-oqVuAfXRKap7fdgcCY5uykM6+R9GqQ8K/uxy9rx7HNQlGYl1kPzQho1wx4JwY8wC"
crossorigin="anonymous"></script>
```

References

Subresource Integrity
https://developer.mozilla.org/en-US/docs/Web/Security/Subresource_Integrity

SRI Hash Generator
https://www.srihash.org/

Insecure HTTP Usage

It was detected that your web application uses HTTP protocol, but doesn't automatically redirect users to HTTPS.

CWE
CWE-16

CVSS2
AV:N/AC:L/Au:N/C:N/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	None
Integrity Impact	None
Availability Impact	None

CVSS3
CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:N/A:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	Required
Scope	Changed
Confidentiality	None
Integrity Impact	None
Availability Impact	None

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	Active
Confidentiality Impact to the Vulnerable System	None
Integrity Impact to the Vulnerable System	None
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

In some circumstances, it could be used for a man-in-the-middle (MitM) attack

http://10.255.112.211/

Request

```
GET / HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0 Safari/537.36
Host: 10.255.112.211
Connection: Keep-alive
```

Recommendation

It's recommended to implement best practices of HTTP Redirection into your web application. Consult web references for more information

References

HTTP Redirections
https://infosec.mozilla.org/guidelines/web_security#http-redirections

WordPress 5.1.x Multiple Vulnerabilities

WordPress is prone to multiple vulnerabilities, including XML External Entity injection and information disclosure vulnerabilities. Exploiting these issues could allow an attacker to obtain sensitive information which could be used to launch further attacks. WordPress versions 5.1.x ranging from 5.1 and up to (and including) 5.1.8 are vulnerable.

CWE

CWE-611

CVSS2

AV:N/AC:L/Au:S/C:P/I:N/A:N/E:POC/RL:OF/RC:C

Access Vector	Network
Access Complexity	Low
Authentication	Single
Confidentiality	Partial
Integrity Impact	None
Availability Impact	None
Exploitability	Proof of concept code
Remediation Level	Official Fix
Report Confidence	Confirmed

CVSS3

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:N/A:N

Base Score	5
Attack Vector	Network
Attack Complexity	Low
Privileges Required	Low
User Interaction	None
Scope	Changed
Confidentiality	Low
Integrity Impact	None
Availability Impact	None

CVSS4

CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:L/VI:N/VA:N/SC:N/S

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	Low
User Interaction	None
Confidentiality Impact to the Vulnerable System	Low
Integrity Impact to the Vulnerable System	None
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

http://10.255.112.211/

wordpress v5.1.1-5.1.1

Recommendation

Update to WordPress version 5.1.9 or latest

References

https://blog.sonarsource.com/wordpress-xxe-security-vulnerability/
https://blog.sonarsource.com/wordpress-xxe-security-vulnerability/

https://github.com/motikan2010/CVE-2021-29447
https://github.com/motikan2010/CVE-2021-29447

https://wordpress.org/support/wordpress-version/version-5-1-9/
https://wordpress.org/support/wordpress-version/version-5-1-9/

A06 Vulnerable and Outdated Components

Components, such as libraries, frameworks, and other software modules, almost always run with full privileges. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications using components with known vulnerabilities may undermine application defenses and enable a range of possible attacks and impacts.

WordPress CVE-2020-28039 Vulnerability

is_protected_meta in wp-includes/meta.php in WordPress before 5.5.2 allows arbitrary file deletion because it does not properly determine whether a meta key is considered protected.

CVSS3
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H

Base Score	9.1
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	None
Integrity Impact	High
Availability Impact	High

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:H/VA:H/SC:N/SI:N/SA:N

Base Score	8.8
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	None
Confidentiality Impact to the Vulnerable System	None
Integrity Impact to the Vulnerable System	High
Availability Impact to the Vulnerable System	High
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

http://10.255.112.211/

wordpress v5.1.1-5.1.1

References

CVE-2020-28039
https://nvd.nist.gov/vuln/detail/CVE-2020-28039

WordPress Deserialization of Untrusted Data Vulnerability

PHPMailer 6.1.8 through 6.4.0 allows object injection through Phar Deserialization via addAttachment with a UNC pathname. NOTE: this is similar to CVE-2018-19296, but arose because 6.1.8 fixed a functionality problem in which UNC pathnames were always considered unreadable by PHPMailer, even in safe contexts. As an unintended side effect, this fix eliminated the code that blocked addAttachment exploitation. WordPress Source: https://wordpress.org/news/2021/05/wordpress-5-7-2-security-release/

CWE
CWE-502

Impact

http://10.255.112.211/

wordpress v5.1.1-5.1.1

http://10.255.112.211/

wordpress v5.1.1-5.1.1

http://10.255.112.211/

wordpress v5.1.1-5.1.1

http://10.255.112.211/

wordpress v5.1.1-5.1.1

References

CVE-2020-36326
https://nvd.nist.gov/vuln/detail/CVE-2020-36326

WordPress Improper Input Validation Vulnerability

wp_kses_bad_protocol in wp-includes/kses.php in WordPress before 5.3.1 mishandles the HTML5 colon named entity, allowing attackers to bypass input sanitization, as demonstrated by the javascript: substring.

CWE
CWE-20

CVSS3
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Base Score	9.8
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	High
Integrity Impact	High
Availability Impact	High

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N

Base Score	8.7
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	Low
User Interaction	None
Confidentiality Impact to the Vulnerable System	High
Integrity Impact to the Vulnerable System	High
Availability Impact to the Vulnerable System	High
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

http://10.255.112.211/

wordpress v5.1.1-5.1.1

http://10.255.112.211/

wordpress v5.1.1-5.1.1

http://10.255.112.211/

wordpress v5.1.1-5.1.1

References

CVE-2019-20041
https://nvd.nist.gov/vuln/detail/CVE-2019-20041

WordPress Improper Privilege Management Vulnerability

WordPress before 5.5.2 allows attackers to gain privileges via XML-RPC.

CWE
CWE-269

CVSS3
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Base Score	9.8
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	High
Integrity Impact	High
Availability Impact	High

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N

Base Score	8.7
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	Low
User Interaction	None
Confidentiality Impact to the Vulnerable System	High
Integrity Impact to the Vulnerable System	High
Availability Impact to the Vulnerable System	High
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

http://10.255.112.211/

wordpress v5.1.1-5.1.1

http://10.255.112.211/

wordpress v5.1.1-5.1.1

http://10.255.112.211/

wordpress v5.1.1-5.1.1

References

CVE-2020-28035
https://nvd.nist.gov/vuln/detail/CVE-2020-28035

WordPress Other Vulnerability

WordPress before 5.8 lacks support for the Update URI plugin header. This makes it easier for remote attackers to execute arbitrary code via a supply-chain attack against WordPress installations that use any plugin for which the slug satisfies the naming constraints of the WordPress.org Plugin Directory but is not yet present in that directory.

CVSS3
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Base Score	9.8
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	High
Integrity Impact	High
Availability Impact	High

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N

Base Score	8.7
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	Low
User Interaction	None
Confidentiality Impact to the Vulnerable System	High
Integrity Impact to the Vulnerable System	High
Availability Impact to the Vulnerable System	High
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

http://10.255.112.211/

wordpress v5.1.1-5.1.1

http://10.255.112.211/

wordpress v5.1.1-5.1.1

http://10.255.112.211/

wordpress v5.1.1-5.1.1

References

CVE-2021-44223
https://nvd.nist.gov/vuln/detail/CVE-2021-44223

WordPress Server-Side Request Forgery (SSRF) Vulnerability

WordPress before 5.2.4 has a Server Side Request Forgery (SSRF) vulnerability because Windows paths are mishandled during certain validation of relative URLs.

CWE
CWE-918

CVSS3
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Base Score	9.8
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	High
Integrity Impact	High
Availability Impact	High

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N

Base Score	8.7
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	Low
User Interaction	None
Confidentiality Impact to the Vulnerable System	High
Integrity Impact to the Vulnerable System	High
Availability Impact to the Vulnerable System	High
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

http://10.255.112.211/

wordpress v5.1.1-5.1.1

http://10.255.112.211/

wordpress v5.1.1-5.1.1

References

CVE-2019-17670
https://nvd.nist.gov/vuln/detail/CVE-2019-17670

WordPress 5.1.x Multiple Vulnerabilities

WordPress is prone to multiple vulnerabilities, including cross-site scripting and SQL injection vulnerabilities. Exploiting these issues could allow an attacker to execute arbitrary script code in the browser of an unsuspecting user in the context of the affected site, allowing the attacker to steal cookie-

based authentication credentials, or to compromise the application, access or modify data or exploit vulnerabilities in the underlying database. WordPress versions 5.1.x ranging from 5.1 and up to (and including) 5.1.13 are vulnerable.

CWE
CWE-89

CVSS2
AV:N/AC:H/Au:S/C:P/I:P/A:P/E:H/RL:OF/RC:C

Access Vector	Network
Access Complexity	High
Authentication	Single
Confidentiality	Partial
Integrity Impact	Partial
Availability Impact	Partial
Exploitability	High
Remediation Level	Official Fix
Report Confidence	Confirmed

CVSS3
CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H

Base Score	8
Attack Vector	Network
Attack Complexity	High
Privileges Required	High
User Interaction	None
Scope	Changed
Confidentiality	High
Integrity Impact	High
Availability Impact	High

CVSS4
CVSS:4.0/AV:N/AC:H/AT:N/PR:H/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N

Base Score	7.5
Attack Vector	Network
Attack Complexity	High
Attack Requirements	None
Privileges Required	High
User Interaction	None
Confidentiality Impact to the Vulnerable System	High
Integrity Impact to the Vulnerable System	High
Availability Impact to the Vulnerable System	High
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

http://10.255.112.211/
wordpress v5.1.1-5.1.1

http://10.255.112.211/
wordpress v5.1.1-5.1.1

http://10.255.112.211/
wordpress v5.1.1-5.1.1

http://10.255.112.211/
wordpress v5.1.1-5.1.1

http://10.255.112.211/
wordpress v5.1.1-5.1.1

http://10.255.112.211/
wordpress v5.1.1-5.1.1

http://10.255.112.211/
wordpress v5.1.1-5.1.1

http://10.255.112.211/
wordpress v5.1.1-5.1.1

http://10.255.112.211/
wordpress v5.1.1-5.1.1

http://10.255.112.211/
wordpress v5.1.1-5.1.1

http://10.255.112.211/
wordpress v5.1.1-5.1.1

http://10.255.112.211/

wordpress v5.1.1-5.1.1

http://10.255.112.211/

wordpress v5.1.1-5.1.1

Recommendation

Update to WordPress version 5.1.14 or latest

References

https://www.wordfence.com/blog/2022/08/wordpress-core-6-0-2-security-maintenance-release-what-you-need-to-know/
https://www.wordfence.com/blog/2022/08/wordpress-core-6-0-2-security-maintenance-release-what-you-need-to-know/

https://wordpress.org/news/2022/08/wordpress-6-0-2-security-and-maintenance-release/
https://wordpress.org/news/2022/08/wordpress-6-0-2-security-and-maintenance-release/

WordPress 5.1.x PHP Object Injection

WordPress is prone to a vulnerability that lets remote attackers inject and execute arbitrary code because the application fails to sanitize user-supplied input before being passed to the unserialize() PHP function. Attackers can possibly exploit this issue to execute arbitrary PHP code within the context of the affected webserver process. WordPress versions 5.1.x ranging from 5.1 and up to (and including) 5.1.9 are vulnerable.

CWE
CWE-915

CVSS2
AV:N/AC:M/Au:N/C:P/I:P/A:P/E:POC/RL:OF/RC:C

Access Vector	Network
Access Complexity	Medium
Authentication	None
Confidentiality	Partial
Integrity Impact	Partial
Availability Impact	Partial
Exploitability	Proof of concept code
Remediation Level	Official Fix
Report Confidence	Confirmed

CVSS3
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Base Score	9.8
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	High
Integrity Impact	High
Availability Impact	High

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/S

Base Score	8.7
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	Low
User Interaction	None
Confidentiality Impact to the Vulnerable System	High
Integrity Impact to the Vulnerable System	High
Availability Impact to the Vulnerable System	High
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

http://10.255.112.211/

wordpress v5.1.1-5.1.1

Recommendation

Update to WordPress version 5.1.10 or latest

References

https://github.com/JamesGeee/CVE-2020-36326
https://github.com/JamesGeee/CVE-2020-36326

https://wordpress.org/support/wordpress-version/version-5-1-10/
https://wordpress.org/support/wordpress-version/version-5-1-10/

WordPress 5.1.x Prototype Pollution

WordPress is prone to a prototype pollution vulnerability. Exploiting this issue could allow an attacker to inject key/value &#65533;properties&#65533; into JavaScript objects, potentially allowing for execution of arbitrary JavaScript in a user&#65533;s session if they can trick that user into clicking a link. WordPress versions 5.1.x ranging from 5.1 and up to (and including) 5.1.12 are vulnerable.

CWE
CWE-1321

CVSS2
AV:N/AC:H/Au:N/C:P/I:P/A:P/E:POC/RL:OF/RC:C

Access Vector	Network
Access Complexity	High
Authentication	None
Confidentiality	Partial
Integrity Impact	Partial
Availability Impact	Partial
Exploitability	Proof of concept code
Remediation Level	Official Fix
Report Confidence	Confirmed

CVSS3
CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L

Base Score	5
Attack Vector	Network
Attack Complexity	High
Privileges Required	None
User Interaction	Required
Scope	Unchanged
Confidentiality	Low
Integrity Impact	Low
Availability Impact	Low

CVSS4
CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:A/VC:L/VI:L/VA:L/SC:N/SI:

Base Score	2.1
Attack Vector	Network
Attack Complexity	High
Attack Requirements	None
Privileges Required	None
User Interaction	Active
Confidentiality Impact to the Vulnerable System	Low
Integrity Impact to the Vulnerable System	Low
Availability Impact to the Vulnerable System	Low
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

http://10.255.112.211/
wordpress v5.1.1-5.1.1

Recommendation

Update to WordPress version 5.1.13 or latest

References

https://github.com/BlackFan/client-side-prototype-pollution/blob/master/pp/jquery-query-object.md
https://github.com/BlackFan/client-side-prototype-pollution/blob/master/pp/jquery-query-object.md

https://wordpress.org/support/wordpress-version/version-5-1-13/
https://wordpress.org/support/wordpress-version/version-5-1-13/

WordPress Access of Resource Using Incompatible Type ('Type Confusion') Vulnerability

WordPress before 5.2.4 does not properly consider type confusion during validation of the referer in the admin pages, possibly leading to CSRF.

CWE
CWE-843

CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Base Score	8.8
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	Required
Scope	Unchanged
Confidentiality	High
Integrity Impact	High
Availability Impact	High

CVSS4

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N

Base Score	8.6
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	Active
Confidentiality Impact to the Vulnerable System	High
Integrity Impact to the Vulnerable System	High
Availability Impact to the Vulnerable System	High
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

http://10.255.112.211/

wordpress v5.1.1-5.1.1

References

CVE-2019-17675
https://nvd.nist.gov/vuln/detail/CVE-2019-17675

WordPress CVE-2019-17673 Vulnerability

WordPress before 5.2.4 is vulnerable to poisoning of the cache of JSON GET requests because certain requests lack a Vary: Origin header.

CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N

Base Score	7.5
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	None
Integrity Impact	High
Availability Impact	None

CVSS4

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:H/VA:N/SC:N/SI:N/SA:N

Base Score	8.7
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	None
Confidentiality Impact to the Vulnerable System	None
Integrity Impact to the Vulnerable System	High
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

http://10.255.112.211/

wordpress v5.1.1-5.1.1

References

CVE-2019-17673
https://nvd.nist.gov/vuln/detail/CVE-2019-17673

WordPress CVE-2020-28033 Vulnerability

WordPress before 5.5.2 mishandles embeds from disabled sites on a multisite network, as demonstrated by allowing a spam embed.

CVSS3
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N

Base Score	7.5
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	None
Integrity Impact	High
Availability Impact	None

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:H/VA:N/SC:N/SI:N/SA:N

Base Score	8.7
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	None
Confidentiality Impact to the Vulnerable System	None
Integrity Impact to the Vulnerable System	High
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

http://10.255.112.211/

wordpress v5.1.1-5.1.1

References

CVE-2020-28033
https://nvd.nist.gov/vuln/detail/CVE-2020-28033

WordPress Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') Vulnerability

WordPress is a free and open-source content management system written in PHP and paired with a MariaDB database. Due to lack of proper sanitization in one of the classes, there's potential for unintended SQL queries to be executed. This has been patched in WordPress version 5.8.3. Older affected versions are also fixed via security release, that go back till 4.1.34. We strongly recommend that you keep auto-updates enabled. There are no known workarounds for this issue.

CWE
CWE-138

CVSS3
CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Base Score	8.8
Attack Vector	Network
Attack Complexity	Low
Privileges Required	Low
User Interaction	None
Scope	Unchanged
Confidentiality	High
Integrity Impact	High
Availability Impact	High

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N

Base Score	9.3
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	None
Confidentiality Impact to the Vulnerable System	High
Integrity Impact to the Vulnerable System	High
Availability Impact to the Vulnerable System	High

Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

http://10.255.112.211/

wordpress v5.1.1-5.1.1

http://10.255.112.211/

wordpress v5.1.1-5.1.1

http://10.255.112.211/

wordpress v5.1.1-5.1.1

http://10.255.112.211/

wordpress v5.1.1-5.1.1

http://10.255.112.211/

wordpress v5.1.1-5.1.1

References

CVE-2022-21664
https://nvd.nist.gov/vuln/detail/CVE-2022-21664

WordPress Missing Authentication for Critical Function Vulnerability

In affected versions of WordPress, some private posts, which were previously public, can result in unauthenticated disclosure under a specific set of conditions. This has been patched in version 5.4.1, along with all the previously affected versions via a minor release (5.3.3, 5.2.6, 5.1.5, 5.0.9, 4.9.14, 4.8.13, 4.7.17, 4.6.18, 4.5.21, 4.4.22, 4.3.23, 4.2.27, 4.1.30, 4.0.30, 3.9.31, 3.8.33, 3.7.33).

CWE
CWE-306

CVSS3
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

Base Score	7.5
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	High
Integrity Impact	None
Availability Impact	None

CVSS4
CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N

Base Score	8.2
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	Present
Privileges Required	None
User Interaction	None
Confidentiality Impact to the Vulnerable System	High
Integrity Impact to the Vulnerable System	None
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

http://10.255.112.211/

wordpress v5.1.1-5.1.1

References

CVE-2020-11028
https://nvd.nist.gov/vuln/detail/CVE-2020-11028

WordPress Server-Side Request Forgery

WordPress is prone to a server-side request forgery vulnerability. An attacker may leverage this issue to make the vulnerable server perform port scanning of hosts in internal or external networks; other attacks are also possible. WordPress versions ranging from 3.7 and up to (and including) 6.1.1 are vulnerable.

CWE
CWE-918

CVSS2
AV:N/AC:H/Au:N/C:P/I:P/A:N/E:H/RL:W/RC:C

Access Vector	Network
Access Complexity	High
Authentication	None
Confidentiality	Partial
Integrity Impact	Partial
Availability Impact	None
Exploitability	High
Remediation Level	Workaround
Report Confidence	Confirmed

CVSS3
CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N

Base Score	4.8
Attack Vector	Network
Attack Complexity	High
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity Impact	Low
Availability Impact	None

CVSS4
CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:N/VC:L/VI:L/VA:N/SC:N/SI:N

Base Score	6.3
Attack Vector	Network
Attack Complexity	High
Attack Requirements	None
Privileges Required	None
User Interaction	None
Confidentiality Impact to the Vulnerable System	Low
Integrity Impact to the Vulnerable System	Low
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

http://10.255.112.211/

wordpress v5.1.1-5.1.1

Recommendation

Block/Turn off access to XMLRPC/pingbacks as per researchers recommandation

References

https://blog.sonarsource.com/wordpress-core-unauthenticated-blind-ssrf/
https://blog.sonarsource.com/wordpress-core-unauthenticated-blind-ssrf/

https://sploitus.com/exploit?id=WPEX-ID:C8814E6E-78B3-4F63-A1D3-6906A84C1F11
https://sploitus.com/exploit?id=WPEX-ID:C8814E6E-78B3-4F63-A1D3-6906A84C1F11

WordPress Uncontrolled Resource Consumption Vulnerability

WordPress through 6.1.1 depends on unpredictable client visits to cause wp-cron.php execution and the resulting security updates, and the source code describes "the scenario where a site may not receive enough visits to execute scheduled tasks in a timely manner," but neither the installation guide nor the security guide mentions this default behavior, or alerts the user about security risks on installations with very few visits.

CWE
CWE-400

CVSS3
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Base Score	7.5
Attack Vector	Network

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:L

Base Score	8.7
Attack Vector	Network

Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	None
Integrity Impact	None
Availability Impact	High

Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	None
Confidentiality Impact to the Vulnerable System	None
Integrity Impact to the Vulnerable System	None
Availability Impact to the Vulnerable System	High
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	Low

Impact

http://10.255.112.211/

wordpress v5.1.1-5.1.1

References

CVE-2023-22622
https://nvd.nist.gov/vuln/detail/CVE-2023-22622

WordPress Weak Password Recovery Mechanism for Forgotten Password Vulnerability

In affected versions of WordPress, a password reset link emailed to a user does not expire upon changing the user password. Access would be needed to the email account of the user by a malicious party for successful execution. This has been patched in version 5.4.1, along with all the previously affected versions via a minor release (5.3.3, 5.2.6, 5.1.5, 5.0.9, 4.9.14, 4.8.13, 4.7.17, 4.6.18, 4.5.21, 4.4.22, 4.3.23, 4.2.27, 4.1.30, 4.0.30, 3.9.31, 3.8.33, 3.7.33).

CWE
CWE-640

CVSS3
CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N

Base Score	8.1
Attack Vector	Network
Attack Complexity	Low
Privileges Required	Low
User Interaction	None
Scope	Unchanged
Confidentiality	High
Integrity Impact	High
Availability Impact	None

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N

Base Score	8.6
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	Low
User Interaction	None
Confidentiality Impact to the Vulnerable System	High
Integrity Impact to the Vulnerable System	High
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

http://10.255.112.211/

wordpress v5.1.1-5.1.1

References

CVE-2020-11027
https://nvd.nist.gov/vuln/detail/CVE-2020-11027

jQuery Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

jQuery before 3.0.0 is vulnerable to Cross-site Scripting (XSS) attacks when a cross-domain Ajax request is performed without the dataType option, causing text/javascript responses to be executed.

CWE
CWE-707

CVSS3
CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

Base Score	6.1
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	Required
Scope	Changed
Confidentiality	Low
Integrity Impact	Low
Availability Impact	None

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:L/SI:L/SA:N

Base Score	5.1
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	Active
Confidentiality Impact to the Vulnerable System	None
Integrity Impact to the Vulnerable System	None
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	Low
Integrity Impact to the Subsequent System	Low
Availability Impact to the Subsequent System	None

Impact

http://10.255.112.211/
jquery v1.12.4-1.12.4

http://10.255.112.211/
jquery v1.12.4-1.12.4

http://10.255.112.211/
jquery v1.12.4-1.12.4

References

CVE-2015-9251
https://nvd.nist.gov/vuln/detail/CVE-2015-9251

JQuery Prototype Pollution Vulnerability

jQuery before 3.4.0, as used in Drupal, Backdrop CMS, and other products, mishandles jQuery.extend(true, {}, ...) because of Object.prototype pollution. If an unsanitized source object contained an enumerable __proto__ property, it could extend the native Object.prototype.

CVSS3
CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

Base Score	6.1
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	Required
Scope	Changed
Confidentiality	Low
Integrity Impact	Low
Availability Impact	None

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:L/SI:L/SA:N

Base Score	5.1
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	Active
Confidentiality Impact to the Vulnerable System	None
Integrity Impact to the Vulnerable System	None
Availability Impact to the Vulnerable System	None

Confidentiality Impact to the Subsequent System	Low
Integrity Impact to the Subsequent System	Low
Availability Impact to the Subsequent System	None

Impact

http://10.255.112.211/

jquery v1.12.4-1.12.4

References

CVE-2019-11358
https://nvd.nist.gov/vuln/detail/CVE-2019-11358

Vulnerable JavaScript libraries

You are using one or more vulnerable JavaScript libraries. One or more vulnerabilities were reported for this version of the library. Consult Attack details and Web References for more information about the affected library and the vulnerabilities that were reported.

CWE
CWE-937

CVSS2
AV:N/AC:L/Au:N/C:P/I:P/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	Partial
Availability Impact	None

CVSS3
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N

Base Score	6.5
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity Impact	Low
Availability Impact	None

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N

Base Score	6.9
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	None
Confidentiality Impact to the Vulnerable System	Low
Integrity Impact to the Vulnerable System	Low
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

Consult References for more information.

http://10.255.112.211/ Confidence: 95%

- jQuery 1.12.4
  - URL: http://10.255.112.211/index.php
  - Detection method: The library's name and version were determined based on its dynamic behavior.
  - CVE-ID: CVE-2015-9251, CVE-2020-11022, CVE-2020-11023
  - Description: Possible Cross Site Scripting via third-party text/javascript responses (1.12.0-1.12.2 mitigation reverted) / In jQuery versions greater than or equal to 1.2 and before 3.5.0, passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0. / In jQuery versions greater than or equal to 1.0.3 and before 3.5.0, passing HTML containing option elements from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.
  - References:
    - https://github.com/jquery/jquery/issues/2432
    - https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/
    - https://mksben.l0.cm/2020/05/jquery3.5.0-xss.html
    - https://jquery.com/upgrade-guide/3.5/
    - https://api.jquery.com/jQuery.htmlPrefilter/
    - https://www.cvedetails.com/cve/CVE-2020-11022/

- https://github.com/advisories/GHSA-gxr4-xjj5-5px2
- https://www.cvedetails.com/cve/CVE-2020-11023/
- https://github.com/advisories/GHSA-jpcq-cgw6-v4j6

Request

```
GET /index.php HTTP/1.1
Referer: http://10.255.112.211/
Cookie: wordpress_test_cookie=WP+Cookie+check
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0 Safari/537.36
Host: 10.255.112.211
Connection: Keep-alive
```

Recommendation

Upgrade to the latest version.

WordPress Cross-Site Request Forgery (CSRF) Vulnerability

WordPress before 5.5.2 allows CSRF attacks that change a theme's background image.

CWE

CWE-352

CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N

Base Score	4.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	Required
Scope	Unchanged
Confidentiality	None
Integrity Impact	Low
Availability Impact	None

CVSS4

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N

Base Score	5.1
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	Active
Confidentiality Impact to the Vulnerable System	None
Integrity Impact to the Vulnerable System	Low
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

http://10.255.112.211/

wordpress v5.1.1-5.1.1

http://10.255.112.211/

wordpress v5.1.1-5.1.1

References

CVE-2020-28040
https://nvd.nist.gov/vuln/detail/CVE-2020-28040

WordPress CVE-2020-25286 Vulnerability

In wp-includes/comment-template.php in WordPress before 5.4.2, comments from a post or page could sometimes be seen in the latest comments even if the post or page was not public.

CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

CVSS4

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:P/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity Impact	None
Availability Impact	None

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	Passive
Confidentiality Impact to the Vulnerable System	Low
Integrity Impact to the Vulnerable System	None
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

http://10.255.112.211/

wordpress v5.1.1-5.1.1

References

CVE-2020-25286
https://nvd.nist.gov/vuln/detail/CVE-2020-25286

WordPress Exposure of Sensitive Information to an Unauthorized Actor Vulnerability

Wordpress is an open source CMS. One of the blocks in the WordPress editor can be exploited in a way that exposes password-protected posts and pages. This requires at least contributor privileges. This has been patched in WordPress 5.7.1, along with the older affected versions via minor releases. It's strongly recommended that you keep auto-updates enabled to receive the fix.

CWE
CWE-200

CVSS3
CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N

Base Score	4.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	Low
User Interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity Impact	None
Availability Impact	None

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	Low
User Interaction	None
Confidentiality Impact to the Vulnerable System	Low
Integrity Impact to the Vulnerable System	None
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

http://10.255.112.211/

wordpress v5.1.1-5.1.1

http://10.255.112.211/

wordpress v5.1.1-5.1.1

References

CVE-2021-29450
https://nvd.nist.gov/vuln/detail/CVE-2021-29450

WordPress Improper Authentication Vulnerability

Improper authentication vulnerability in WordPress versions prior to 6.0.3 allows a remote unauthenticated attacker to obtain the email address of the user who posted a blog using the WordPress Post by Email Feature. The developer also provides new patched releases for all versions since 3.7.

CWE
CWE-287

CVSS3
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity Impact	None
Availability Impact	None

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:P/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	Passive
Confidentiality Impact to the Vulnerable System	Low
Integrity Impact to the Vulnerable System	None
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

http://10.255.112.211/
wordpress v5.1.1-5.1.1

References

CVE-2022-43504
https://nvd.nist.gov/vuln/detail/CVE-2022-43504

WordPress Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') Vulnerability

WordPress Core is vulnerable to Directory Traversal in versions up to, and including, 6.2, via the 'wp_lang' parameter. This allows unauthenticated attackers to access and load arbitrary translation files. In cases where an attacker is able to upload a crafted translation file onto the site, such as via an upload form, this could be also used to perform a Cross-Site Scripting attack.

CWE
CWE-22

CVSS3
CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

Base Score	6.1
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	Required
Scope	Changed
Confidentiality	Low

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:L/SI:L/SA:N

Base Score	5.1
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	Active
Confidentiality Impact to the Vulnerable System	None

Integrity Impact	Low
Availability Impact	None

Integrity Impact to the Vulnerable System	None
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	Low
Integrity Impact to the Subsequent System	Low
Availability Impact to the Subsequent System	None

Impact

http://10.255.112.211/

wordpress v5.1.1-5.1.1

http://10.255.112.211/

wordpress v5.1.1-5.1.1

References

CVE-2023-2745
https://nvd.nist.gov/vuln/detail/CVE-2023-2745

WordPress Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

WordPress before 5.2.3 allows reflected XSS in the dashboard.

CWE
CWE-707

CVSS3
CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

Base Score	6.1
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	Required
Scope	Changed
Confidentiality	Low
Integrity Impact	Low
Availability Impact	None

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:L/SI:L/SA:N

Base Score	5.1
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	Active
Confidentiality Impact to the Vulnerable System	None
Integrity Impact to the Vulnerable System	None
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	Low
Integrity Impact to the Subsequent System	Low
Availability Impact to the Subsequent System	None

Impact

http://10.255.112.211/

wordpress v5.1.1-5.1.1

http://10.255.112.211/

wordpress v5.1.1-5.1.1

http://10.255.112.211/

wordpress v5.1.1-5.1.1

http://10.255.112.211/

wordpress v5.1.1-5.1.1

http://10.255.112.211/

wordpress v5.1.1-5.1.1

http://10.255.112.211/

wordpress v5.1.1-5.1.1

http://10.255.112.211/

wordpress v5.1.1-5.1.1

http://10.255.112.211/

wordpress v5.1.1-5.1.1

http://10.255.112.211/

wordpress v5.1.1-5.1.1

http://10.255.112.211/

wordpress v5.1.1-5.1.1

http://10.255.112.211/

wordpress v5.1.1-5.1.1

http://10.255.112.211/

wordpress v5.1.1-5.1.1

http://10.255.112.211/

wordpress v5.1.1-5.1.1

http://10.255.112.211/

wordpress v5.1.1-5.1.1

http://10.255.112.211/

wordpress v5.1.1-5.1.1

http://10.255.112.211/

wordpress v5.1.1-5.1.1

http://10.255.112.211/

wordpress v5.1.1-5.1.1

http://10.255.112.211/

wordpress v5.1.1-5.1.1

http://10.255.112.211/

wordpress v5.1.1-5.1.1

http://10.255.112.211/

wordpress v5.1.1-5.1.1

http://10.255.112.211/

wordpress v5.1.1-5.1.1

http://10.255.112.211/

wordpress v5.1.1-5.1.1

http://10.255.112.211/

wordpress v5.1.1-5.1.1

http://10.255.112.211/

wordpress v5.1.1-5.1.1

http://10.255.112.211/

wordpress v5.1.1-5.1.1

http://10.255.112.211/

wordpress v5.1.1-5.1.1

References

CVE-2019-16221
https://nvd.nist.gov/vuln/detail/CVE-2019-16221

WordPress Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) Vulnerability

In affected versions of WordPress, authenticated users with upload permissions (like authors) are able to inject JavaScript into some media file attachment pages in a certain way. This can lead to script execution in the context of a higher privileged user when the file is viewed by them. This has been patched in version 5.4.2, along with all the previously affected versions via a minor release (5.3.4, 5.2.7, 5.1.6, 5.0.10, 4.9.15, 4.8.14, 4.7.18, 4.6.19, 4.5.22, 4.4.23, 4.3.24, 4.2.28, 4.1.31, 4.0.31, 3.9.32, 3.8.34, 3.7.34).

CWE
CWE-707

CVSS3
CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:N/I:H/A:N

Base Score	6.8
Attack Vector	Network
Attack Complexity	Low
Privileges Required	Low
User Interaction	Required
Scope	Changed
Confidentiality	None
Integrity Impact	High
Availability Impact	None

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:A/VC:N/VI:H/VA:N/SC:N/SI:N/SA:N

Base Score	6.8
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	Low
User Interaction	Active
Confidentiality Impact to the Vulnerable System	None
Integrity Impact to the Vulnerable System	High
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

http://10.255.112.211/

wordpress v5.1.1-5.1.1

http://10.255.112.211/

wordpress v5.1.1-5.1.1

References

CVE-2020-4047
https://nvd.nist.gov/vuln/detail/CVE-2020-4047

WordPress Time-of-check Time-of-use (TOCTOU) Race Condition Vulnerability

WordPress is affected by an unauthenticated blind SSRF in the pingback feature. Because of a TOCTOU race condition between the validation checks and the HTTP request, attackers can reach internal hosts that are explicitly forbidden.

CWE
CWE-367

CVSS3

CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N

Base Score	5.9
Attack Vector	Network
Attack Complexity	High
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	High
Integrity Impact	None
Availability Impact	None

CVSS4

CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N

Base Score	8.2
Attack Vector	Network
Attack Complexity	High
Attack Requirements	None
Privileges Required	None
User Interaction	None
Confidentiality Impact to the Vulnerable System	High
Integrity Impact to the Vulnerable System	None
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

http://10.255.112.211/

wordpress v5.1.1-5.1.1

References

CVE-2022-3590
https://nvd.nist.gov/vuln/detail/CVE-2022-3590

WordPress URL Redirection to Untrusted Site ('Open Redirect') Vulnerability

In affected versions of WordPress, due to an issue in wp_validate_redirect() and URL sanitization, an arbitrary external link can be crafted leading to unintended/open redirect when clicked. This has been patched in version 5.4.2, along with all the previously affected versions via a minor release (5.3.4, 5.2.7, 5.1.6, 5.0.10, 4.9.15, 4.8.14, 4.7.18, 4.6.19, 4.5.22, 4.4.23, 4.3.24, 4.2.28, 4.1.31, 4.0.31, 3.9.32, 3.8.34, 3.7.34).

CWE

CWE-601

CVSS3

CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:H/A:N

Base Score	5.7
Attack Vector	Network
Attack Complexity	Low
Privileges Required	Low
User Interaction	Required
Scope	Unchanged
Confidentiality	None
Integrity Impact	High
Availability Impact	None

CVSS4

CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:A/VC:N/VI:H/VA:N/SC:N/SI:N/SA:N

Base Score	6.8
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	Low
User Interaction	Active
Confidentiality Impact to the Vulnerable System	None
Integrity Impact to the Vulnerable System	High
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

http://10.255.112.211/

wordpress v5.1.1-5.1.1

http://10.255.112.211/

wordpress v5.1.1-5.1.1

References

CVE-2020-4048
https://nvd.nist.gov/vuln/detail/CVE-2020-4048

WordPress Authentication Bypass Using an Alternate Path or Channel Vulnerability

In affected versions of WordPress, misuse of the `set-screen-option` filter's return value allows arbitrary user meta fields to be saved. It does require an admin to install a plugin that would misuse the filter. Once installed, it can be leveraged by low privileged users. This has been patched in version 5.4.2, along with all the previously affected versions via a minor release (5.3.4, 5.2.7, 5.1.6, 5.0.10, 4.9.15, 4.8.14, 4.7.18, 4.6.19, 4.5.22, 4.4.23, 4.3.24, 4.2.28, 4.1.31, 4.0.31, 3.9.32, 3.8.34, 3.7.34).

CWE
CWE-288

CVSS3
CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:L/A:N

Base Score	3.1
Attack Vector	Network
Attack Complexity	High
Privileges Required	Low
User Interaction	None
Scope	Unchanged
Confidentiality	None
Integrity Impact	Low
Availability Impact	None

CVSS4
CVSS:4.0/AV:N/AC:H/AT:N/PR:L/UI:N/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N

Base Score	2.3
Attack Vector	Network
Attack Complexity	High
Attack Requirements	None
Privileges Required	Low
User Interaction	None
Confidentiality Impact to the Vulnerable System	None
Integrity Impact to the Vulnerable System	Low
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

http://10.255.112.211/

wordpress v5.1.1-5.1.1

References

CVE-2020-4050
https://nvd.nist.gov/vuln/detail/CVE-2020-4050

A07 Identification and Authentication Failures

Application functions related to authentication and session management are often implemented incorrectly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities.

SSL/TLS Not Implemented

This scan target was connected to over an unencrypted connection. A potential attacker can intercept and modify data sent and received from this site.

CWE
CWE-319

CVSS2

AV:N/AC:M/Au:N/C:P/I:P/A:N

Access Vector	Network
Access Complexity	Medium
Authentication	None
Confidentiality	Partial
Integrity Impact	Partial
Availability Impact	None

CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N

Base Score	5.4
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	Required
Scope	Unchanged
Confidentiality	Low
Integrity Impact	Low
Availability Impact	None

CVSS4

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N

Base Score	5.1
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	Active
Confidentiality Impact to the Vulnerable System	Low
Integrity Impact to the Vulnerable System	Low
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

Possible information disclosure.

http://10.255.112.211/ Verified

Request

```
GET / HTTP/1.1
Referer: http://10.255.112.211/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0 Safari/537.36
Host: 10.255.112.211
Connection: Keep-alive
```

Recommendation

The site should send and receive data over a secure (HTTPS) connection.

WordPress username enumeration

If permalinks are enabled, in many WordPress installations it is possible to enumerate all the WordPress usernames iterating through the author archives. Whenever a post is published, the username or alias is shown as the author. For example, the URL http://site.com/?author=1 will show all the posts from user id 1. Attackers can abuse this functionality to figure out which usernames are available on the site.

CWE

CWE-200

CVSS2

AV:N/AC:L/Au:N/C:P/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	None
Availability Impact	None

CVSS3

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity Impact	None
Availability Impact	None

CVSS4

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:P/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	Passive
Confidentiality Impact to the Vulnerable System	Low
Integrity Impact to the Vulnerable System	None
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

An attacker can enumerate the WordPress usernames and use this information to conduct brute-force attacks against passwords for these known usernames.

http://10.255.112.211/

List of WordPress users for {'_nativeUrl': {'password': '', 'username': '', 'search': '', 'protocol': 'http', 'port': '', 'path': '/', 'origin': 'http://10.255.112.211', 'href': 'http://10.255.112.211/', 'hostname': '10.255.112.211', 'host': '10.255.112.211', 'hash': ''}}:

['admin']

Request

```
POST //wp-login.php HTTP/1.1
Content-type: application/x-www-form-urlencoded
Cookie: wordpress_test_cookie=WP+Cookie+check
Content-Length: 28
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0 Safari/537.36
Host: 10.255.112.211
Connection: Keep-alive

log=10&pwd=z&wp-submit=Login
```

Recommendation

You can use an .htaccess rewrite rule to prevent this disclosure but you should also be sure to use nicknames to avoid disclosing usernames.

```
# Stop WordPress username enumeration vulnerability
RewriteCond %{REQUEST_URI} ^/$
RewriteCond %{QUERY_STRING} ^/?author=([0-9]*)
RewriteRule ^(.*)$ http://yoursite.com/somepage/? [L,R=301]
```

WordPress default administrator account

By default WordPress creates an administrator user account named **admin**. Using the default Admin WordPress Account, hackers can easily launch a brute force attack against it. In order to help deter this type of attack, you should change your default WordPress administrator username to something more difficult to guess.

CWE
CWE-16

CVSS2
AV:N/AC:L/Au:N/C:N/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	None
Integrity Impact	None
Availability Impact	None

CVSS3
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	None
Integrity Impact	None
Availability Impact	None

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	None
Confidentiality Impact to the Vulnerable System	None
Integrity Impact to the Vulnerable System	None
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

No impact is associated with this vulnerability.

http://10.255.112.211/wp-login.php

Request

```
POST //wp-login.php HTTP/1.1
Content-type: application/x-www-form-urlencoded
Cookie: wordpress_test_cookie=WP+Cookie+check
Content-Length: 41
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0 Safari/537.36
Host: 10.255.112.211
Connection: Keep-alive

log=admin&pwd=testingtest&wp-submit=Login
```

Recommendation

Change the default WordPress administrator username to something more difficult to guess. Consult web references for more information.

References

OWASP Wordpress Security Implementation Guideline
https://www.owasp.org/index.php/OWASP_Wordpress_Security_Implementation_Guideline#Remove_or_change_the_default_administrator_account

Your WordPress Installation Is Using the Default Admin Account
https://www.acunetix.com/blog/wordpress-security/wordpress-default-admin-account/

Change WordPress admin username for security
https://www.inmotionhosting.com/support/website/wordpress/change-wordpress-admin-username-for-security

WordPress admin accessible without HTTP authentication

It's recommended to restrict access to the WordPress administration dashboard using HTTP authentication. Password protecting your WordPress admin dashboard through a layer of HTTP authentication is an effective measure to thwart attackers attempting to guess user's passwords. Additionally, if attackers manage to steal a user's password, they will need to get past HTTP authentication in order to gain access to WordPress login form.

CWE
CWE-16

CVSS2
AV:N/AC:L/Au:N/C:N/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	None
Integrity Impact	None
Availability Impact	None

CVSS3
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	None
Integrity Impact	None
Availability Impact	None

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	None
Confidentiality Impact to the Vulnerable System	None
Integrity Impact to the Vulnerable System	None
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

No impact is associated with this vulnerability.

http://10.255.112.211/wp-admin/

Request

```
GET /wp-admin/ HTTP/1.1
Cookie: wordpress_test_cookie=WP+Cookie+check
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0 Safari/537.36
Host: 10.255.112.211
Connection: Keep-alive
```

Recommendation

Add server-side password protection (such as BasicAuth) to the /wp-admin/ directory. Consult web references for more information.

References

Securing wp-admin
https://codex.wordpress.org/Hardening_WordPress

WordPress Security Tips Part 5 | Restrict Access to wp-admin Directory
https://www.acunetix.com/blog/articles/wordpress-security-wpadmin-directory/

WordPress Improper Authentication Vulnerability

Improper authentication vulnerability in WordPress versions prior to 6.0.3 allows a remote unauthenticated attacker to obtain the email address of the user who posted a blog using the WordPress Post by Email Feature. The developer also provides new patched releases for all versions since 3.7.

CWE
CWE-287

CVSS3
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity Impact	None
Availability Impact	None

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:P/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	Passive
Confidentiality Impact to the Vulnerable System	Low
Integrity Impact to the Vulnerable System	None
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

http://10.255.112.211/

wordpress v5.1.1-5.1.1

References

CVE-2022-43504
https://nvd.nist.gov/vuln/detail/CVE-2022-43504

WordPress Authentication Bypass Using an Alternate Path or Channel Vulnerability

In affected versions of WordPress, misuse of the `set-screen-option` filter's return value allows arbitrary user meta fields to be saved. It does require an admin to install a plugin that would misuse the filter. Once installed, it can be leveraged by low privileged users. This has been patched in version 5.4.2, along with all the previously affected versions via a minor release (5.3.4, 5.2.7, 5.1.6, 5.0.10, 4.9.15, 4.8.14, 4.7.18, 4.6.19, 4.5.22, 4.4.23, 4.3.24, 4.2.28, 4.1.31, 4.0.31, 3.9.32, 3.8.34, 3.7.34).

CWE
CWE-288

CVSS3
CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:L/A:N

Base Score	3.1
Attack Vector	Network

CVSS4
CVSS:4.0/AV:N/AC:H/AT:N/PR:L/UI:N/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N

Base Score	2.3
Attack Vector	Network

Attack Complexity	High
Privileges Required	Low
User Interaction	None
Scope	Unchanged
Confidentiality	None
Integrity Impact	Low
Availability Impact	None

Attack Complexity	High
Attack Requirements	None
Privileges Required	Low
User Interaction	None
Confidentiality Impact to the Vulnerable System	None
Integrity Impact to the Vulnerable System	Low
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

http://10.255.112.211/

wordpress v5.1.1-5.1.1

References

CVE-2020-4050
https://nvd.nist.gov/vuln/detail/CVE-2020-4050

WordPress Missing Authentication for Critical Function Vulnerability

In affected versions of WordPress, some private posts, which were previously public, can result in unauthenticated disclosure under a specific set of conditions. This has been patched in version 5.4.1, along with all the previously affected versions via a minor release (5.3.3, 5.2.6, 5.1.5, 5.0.9, 4.9.14, 4.8.13, 4.7.17, 4.6.18, 4.5.21, 4.4.22, 4.3.23, 4.2.27, 4.1.30, 4.0.30, 3.9.31, 3.8.33, 3.7.33).

CWE
CWE-306

CVSS3
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

Base Score	7.5
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	High
Integrity Impact	None
Availability Impact	None

CVSS4
CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N

Base Score	8.2
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	Present
Privileges Required	None
User Interaction	None
Confidentiality Impact to the Vulnerable System	High
Integrity Impact to the Vulnerable System	None
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

http://10.255.112.211/

wordpress v5.1.1-5.1.1

References

CVE-2020-11028
https://nvd.nist.gov/vuln/detail/CVE-2020-11028

WordPress XML-RPC authentication brute force

WordPress provides an XML-RPC interface via the xmlrpc.php script. XML-RPC is remote procedure calling using HTTP as the transport and XML as the encoding. An attacker can abuse this interface to brute force authentication credentials using API calls such as **wp.getUsersBlogs**.

CWE
CWE-521

CVSS2
AV:N/AC:L/Au:N/C:P/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	None
Availability Impact	None

CVSS3
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:N/A:N

Base Score	5.8
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Changed
Confidentiality	Low
Integrity Impact	None
Availability Impact	None

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N

Base Score	6.9
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	None
Confidentiality Impact to the Vulnerable System	Low
Integrity Impact to the Vulnerable System	None
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

An attacker can brute force the authentication credentials for your WordPress blog.

http://10.255.112.211/xmlrpc.php

Pattern found:

```
<value><string>Incorrect username or password.</string></value>
```

Request

```
POST //xmlrpc.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Cookie: wordpress_test_cookie=WP+Cookie+check
Content-Length: 264
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0 Safari/537.36
Host: 10.255.112.211
Connection: Keep-alive

<?xml version="1.0" encoding="iso-8859-1"?>
<methodCall>
<methodName>wp.getUsersBlogs</methodName>
<params>
<param><value><string>admin</string></value></param>
<param><value><string>8947589543789543753498 7</string></value>
</param>
</params>
</methodCall>
```

Recommendation

It is possible to disable the XML-RPC script if you do not want to use it. Consult references for a WordPress plugin that does that. If you don't want to disable XML-RPC you can monitor for XML-RPC authentication failures with a Web Application Firewall like ModSecurity.

References

WordPress XML-RPC Brute Force Scanning
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/honeypot-alert-wordpress-xml-rpc-brute-force-scanning/

Prevent XMLRPC
https://wordpress.org/plugins/prevent-xmlrpc/

WordPress brute force attack via wp.getUsersBlogs
https://isc.sans.edu/diary/+WordPress+brute+force+attack+via+wp.getUsersBlogs/18427

WordPress Weak Password Recovery Mechanism for Forgotten Password Vulnerability

In affected versions of WordPress, a password reset link emailed to a user does not expire upon changing the user password. Access would be needed to the email account of the user by a malicious party for successful execution. This has been patched in version 5.4.1, along with all the previously affected versions via a minor release (5.3.3, 5.2.6, 5.1.5, 5.0.9, 4.9.14, 4.8.13, 4.7.17, 4.6.18, 4.5.21, 4.4.22, 4.3.23, 4.2.27, 4.1.30, 4.0.30, 3.9.31, 3.8.33, 3.7.33).

CWE
CWE-640

CVSS3
CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N

Base Score	8.1
Attack Vector	Network
Attack Complexity	Low
Privileges Required	Low
User Interaction	None
Scope	Unchanged
Confidentiality	High
Integrity Impact	High
Availability Impact	None

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N

Base Score	8.6
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	Low
User Interaction	None
Confidentiality Impact to the Vulnerable System	High
Integrity Impact to the Vulnerable System	High
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

http://10.255.112.211/
wordpress v5.1.1-5.1.1

References

CVE-2020-11027
https://nvd.nist.gov/vuln/detail/CVE-2020-11027

A08 Software and Data Integrity Failures

Software and data integrity failures relate to code and infrastructure that does not protect against integrity violations. An example of this is where an application relies upon plugins, libraries, or modules from untrusted sources, repositories, and content delivery networks (CDNs). An insecure CI/CD pipeline can introduce the potential for unauthorized access, malicious code, or system compromise. Lastly, many applications now include auto-update functionality, where updates are downloaded without sufficient integrity verification and applied to the previously trusted application. Attackers could potentially upload their own updates to be distributed and run on all installations. Another example is where objects or data are encoded or serialized into a structure that an attacker can see and modify is vulnerable to insecure deserialization.

WordPress Deserialization of Untrusted Data Vulnerability

PHPMailer 6.1.8 through 6.4.0 allows object injection through Phar Deserialization via addAttachment with a UNC pathname. NOTE: this is similar to CVE-2018-19296, but arose because 6.1.8 fixed a functionality problem in which UNC pathnames were always considered unreadable by PHPMailer, even in safe contexts. As an unintended side effect, this fix eliminated the code that blocked addAttachment exploitation. WordPress Source: https://wordpress.org/news/2021/05/wordpress-5-7-2-security-release/

CWE
CWE-502

Impact

http://10.255.112.211/

wordpress v5.1.1-5.1.1

http://10.255.112.211/

wordpress v5.1.1-5.1.1

http://10.255.112.211/

wordpress v5.1.1-5.1.1

http://10.255.112.211/

wordpress v5.1.1-5.1.1

References

CVE-2020-36326
https://nvd.nist.gov/vuln/detail/CVE-2020-36326

WordPress 5.1.x Multiple Vulnerabilities

WordPress is prone to multiple vulnerabilities, including cross-site scripting, privilege escalation, security bypass, Denial of Service and PHP object injection vulnerabilities. Exploiting these issues could allow an attacker to execute arbitrary script code in the browser of an unsuspecting user in the context of the affected site, allowing the attacker to steal cookie-based authentication credentials and launch other attacks, to bypass the expected capabilities check, to perform otherwise restricted actions and subsequently delete arbitrary files, to deny service to legitimate users, or to possibly execute arbitrary PHP code within the context of the affected webserver process. WordPress versions 5.1.x ranging from 5.1 and up to (and including) 5.1.6 are vulnerable.

CWE
CWE-502

CVSS2
AV:N/AC:M/Au:S/C:P/I:P/A:P/E:H/RL:OF/RC:C

Access Vector	Network
Access Complexity	Medium
Authentication	Single
Confidentiality	Partial
Integrity Impact	Partial
Availability Impact	Partial
Exploitability	High
Remediation Level	Official Fix
Report Confidence	Confirmed

CVSS3
CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:L

Base Score	6.5
Attack Vector	Network
Attack Complexity	Low
Privileges Required	Low
User Interaction	Required
Scope	Changed
Confidentiality	Low
Integrity Impact	Low
Availability Impact	Low

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:A/VC:L/VI:L/VA:L/SC:N/SI:N/SA

Base Score	4.8
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	Low
User Interaction	Active
Confidentiality Impact to the Vulnerable System	Low
Integrity Impact to the Vulnerable System	Low
Availability Impact to the Vulnerable System	Low
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

http://10.255.112.211/

wordpress v5.1.1-5.1.1

http://10.255.112.211/

wordpress v5.1.1-5.1.1

Recommendation

Update to WordPress version 5.1.7 or latest

References

https://blog.sucuri.net/2020/10/reflected-xss-in-wordpress-v5-5-1-and-lower.html
https://blog.sucuri.net/2020/10/reflected-xss-in-wordpress-v5-5-1-and-lower.html

https://blog.wpscan.com/2020/10/30/wordpress-5.5.2-security-release.html
https://blog.wpscan.com/2020/10/30/wordpress-5.5.2-security-release.html

https://threatpost.com/wordpress-patches-rce-bug/160812/
https://threatpost.com/wordpress-patches-rce-bug/160812/

https://wordpress.org/support/wordpress-version/version-5-1-7/
https://wordpress.org/support/wordpress-version/version-5-1-7/

Subresource Integrity (SRI) Not Implemented

Subresource Integrity (SRI) is a security feature that enables browsers to verify that third-party resources they fetch (for example, from a CDN) are delivered without unexpected manipulation. It works by allowing developers to provide a cryptographic hash that a fetched file must match.

Third-party resources (such as scripts and stylesheets) can be manipulated. An attacker that has access or has hacked the hosting CDN can manipulate or replace the files. SRI allows developers to specify a base64-encoded cryptographic hash of the resource to be loaded. The integrity attribute containing the hash is then added to the <script> HTML element tag. The integrity string consists of a base64-encoded hash, followed by a prefix that depends on the hash algorithm. This prefix can either be sha256, sha384 or sha512.

The script loaded from the external URL specified in the Details section doesn't implement Subresource Integrity (SRI). It's recommended to implement Subresource Integrity (SRI) for all the scripts loaded from external hosts.

CWE
CWE-830

CVSS2
AV:N/AC:L/Au:N/C:N/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	None
Integrity Impact	None
Availability Impact	None

CVSS3
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Changed
Confidentiality	None
Integrity Impact	None
Availability Impact	None

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N

Base Score	6.9
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	None
Confidentiality Impact to the Vulnerable System	None
Integrity Impact to the Vulnerable System	Low
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

An attacker that has access or has hacked the hosting CDN can manipulate or replace the files.

http://10.255.112.211/index.php

Pages where SRI is not implemented:

- http://10.255.112.211/index.php
  Script SRC: **http://wordy/wp-includes/js/jquery/jquery.js?ver=1.12.4**

Request

```
GET /index.php HTTP/1.1
Referer: http://10.255.112.211/
Cookie: wordpress_test_cookie=WP+Cookie+check
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0 Safari/537.36
Host: 10.255.112.211
Connection: Keep-alive
```

Recommendation

Use the SRI Hash Generator link (from the References section) to generate a <script> element that implements Subresource Integrity (SRI).

For example, you can use the following <script> element to tell a browser that before executing the https://example.com/example-framework.js script, the browser must first compare the script to the expected hash, and verify that there's a match.

```
<script src="https://example.com/example-framework.js"
integrity="sha384-oqVuAfXRKap7fdgcCY5uykM6+R9GqQ8K/uxy9rx7HNQlGYl1kPzQho1wx4JwY8wC"
crossorigin="anonymous"></script>
```

References

Subresource Integrity
https://developer.mozilla.org/en-US/docs/Web/Security/Subresource_Integrity

SRI Hash Generator
https://www.srihash.org/

WordPress 5.1.x PHP Object Injection

WordPress is prone to a vulnerability that lets remote attackers inject and execute arbitrary code because the application fails to sanitize user-supplied input before being passed to the unserialize() PHP function. Attackers can possibly exploit this issue to execute arbitrary PHP code within the context of the affected webserver process. WordPress versions 5.1.x ranging from 5.1 and up to (and including) 5.1.9 are vulnerable.

CWE
CWE-915

CVSS2
AV:N/AC:M/Au:N/C:P/I:P/A:P/E:POC/RL:OF/RC:C

Access Vector	Network
Access Complexity	Medium
Authentication	None
Confidentiality	Partial
Integrity Impact	Partial
Availability Impact	Partial
Exploitability	Proof of concept code
Remediation Level	Official Fix
Report Confidence	Confirmed

CVSS3
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Base Score	9.8
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	High
Integrity Impact	High
Availability Impact	High

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/S

Base Score	8.7
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	Low
User Interaction	None
Confidentiality Impact to the Vulnerable System	High
Integrity Impact to the Vulnerable System	High
Availability Impact to the Vulnerable System	High
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

http://10.255.112.211/

wordpress v5.1.1-5.1.1

Recommendation

Update to WordPress version 5.1.10 or latest

References

https://github.com/JamesGeee/CVE-2020-36326
https://github.com/JamesGeee/CVE-2020-36326

https://wordpress.org/support/wordpress-version/version-5-1-10/
https://wordpress.org/support/wordpress-version/version-5-1-10/

A09 Security Logging and Monitoring Failures

Insufficient logging and monitoring, coupled with missing or ineffective integration with incident response, allows attackers to further attack systesm, maintain persistence, pivot to more systems, and tamper, extract, or destroy data. Most breach studies show time to detect a breach is over 200 days, typically detected by external parties rather than internal processes or monitoring.

No alerts in this category

A10 Server-Side Request Forgery

SSRF flaws occur whenever a web application is fetching a remote resource without validating the user-supplied URL. It allows an attacker to coerce the application to send a crafted request to an unexpected destination, even when protected by a firewall, VPN, or another type of network access control list (ACL).

WordPress Server-Side Request Forgery (SSRF) Vulnerability

WordPress before 5.2.4 has a Server Side Request Forgery (SSRF) vulnerability because Windows paths are mishandled during certain validation of relative URLs.

CWE
CWE-918

CVSS3
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Base Score	9.8
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	High
Integrity Impact	High
Availability Impact	High

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N

Base Score	8.7
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	Low
User Interaction	None
Confidentiality Impact to the Vulnerable System	High
Integrity Impact to the Vulnerable System	High
Availability Impact to the Vulnerable System	High
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

http://10.255.112.211/
wordpress v5.1.1-5.1.1

http://10.255.112.211/
wordpress v5.1.1-5.1.1

References

CVE-2019-17670
https://nvd.nist.gov/vuln/detail/CVE-2019-17670

WordPress 5.1.x Multiple Vulnerabilities

WordPress is prone to multiple vulnerabilities, including cross-site scripting, security bypass, or server-side request forgery vulnerabilities. Exploiting these issues could allow an attacker to execute arbitrary script code in the browser of an unsuspecting user in the context of the affected site, allowing the attacker to steal cookie-based authentication credentials, to bypass certain security restrictions and perform unauthorized actions, or to make the

vulnerable server perform port scanning of hosts in internal or external networks. WordPress versions 5.1.x ranging from 5.1 and up to (and including) 5.1.2 are vulnerable.

CWE
CWE-918

CVSS2
AV:N/AC:M/Au:N/C:P/I:P/A:N/E:POC/RL:OF/RC:C

Access Vector	Network
Access Complexity	Medium
Authentication	None
Confidentiality	Partial
Integrity Impact	Partial
Availability Impact	None
Exploitability	Proof of concept code
Remediation Level	Official Fix
Report Confidence	Confirmed

CVSS3
CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

Base Score	6.1
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	Required
Scope	Changed
Confidentiality	Low
Integrity Impact	Low
Availability Impact	None

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:L/S

Base Score	5.1
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	Active
Confidentiality Impact to the Vulnerable System	None
Integrity Impact to the Vulnerable System	None
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	Low
Integrity Impact to the Subsequent System	Low
Availability Impact to the Subsequent System	None

Impact

http://10.255.112.211/

wordpress v5.1.1-5.1.1

Recommendation

Update to WordPress version 5.1.3 or latest

References

https://blog.wpscan.org/wordpress/security/release/2019/10/15/wordpress-524-security-release-breakdown.html
https://blog.wpscan.org/wordpress/security/release/2019/10/15/wordpress-524-security-release-breakdown.html

https://0day.work/proof-of-concept-for-wordpress-5-2-3-viewing-unauthenticated-posts/
https://0day.work/proof-of-concept-for-wordpress-5-2-3-viewing-unauthenticated-posts/

https://blog.ripstech.com/2020/wordpress-hardening-bypass/
https://blog.ripstech.com/2020/wordpress-hardening-bypass/

https://wordpress.org/support/wordpress-version/version-5-1-3/
https://wordpress.org/support/wordpress-version/version-5-1-3/

https://wordpress.org/news/2019/11/wordpress-5-2-4-update/
https://wordpress.org/news/2019/11/wordpress-5-2-4-update/

WordPress Server-Side Request Forgery

WordPress is prone to a server-side request forgery vulnerability. An attacker may leverage this issue to make the vulnerable server perform port scanning of hosts in internal or external networks; other attacks are also possible. WordPress versions ranging from 3.7 and up to (and including) 6.1.1 are vulnerable.

CWE
CWE-918

CVSS2
AV:N/AC:H/Au:N/C:P/I:P/A:N/E:H/RL:W/RC:C

Access Vector	Network
Access Complexity	High
Authentication	None
Confidentiality	Partial

CVSS3
CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N

Base Score	4.8
Attack Vector	Network
Attack Complexity	High
Privileges Required	None

CVSS4
CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:N/VC:L/VI:L/VA:N/SC:N/SI:N

Base Score	6.3
Attack Vector	Network
Attack Complexity	High
Attack Requirements	None

Integrity Impact	Partial
Availability Impact	None
Exploitability	High
Remediation Level	Workaround
Report Confidence	Confirmed

User Interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity Impact	Low
Availability Impact	None

Privileges Required	None
User Interaction	None
Confidentiality Impact to the Vulnerable System	Low
Integrity Impact to the Vulnerable System	Low
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

http://10.255.112.211/

wordpress v5.1.1-5.1.1

Recommendation

Block/Turn off access to XMLRPC/pingbacks as per researchers recommandation

References

https://blog.sonarsource.com/wordpress-core-unauthenticated-blind-ssrf/
https://blog.sonarsource.com/wordpress-core-unauthenticated-blind-ssrf/

https://sploitus.com/exploit?id=WPEX-ID:C8814E6E-78B3-4F63-A1D3-6906A84C1F11
https://sploitus.com/exploit?id=WPEX-ID:C8814E6E-78B3-4F63-A1D3-6906A84C1F11

Coverage

- http://10.255.112.211
  - icons
  - wp-admin
    - css
      - install.css
    - images
    - includes
    - js
    - user
    - import.php
    - install.php
    - update-core.php
    - upgrade.php
  - wp-content
    - plugins
    - themes
  - wp-includes
    - blocks
      - archives.php
      - block.php
      - categories.php
      - latest-comments.php
      - latest-posts.php
      - shortcode.php
    - certificates
    - css
    - customize
    - fonts
    - ID3
      - getid3.lib.php
      - getid3.php
      - license.commercial.txt
      - license.txt
      - module.audio-video.asf.php
      - module.audio-video.flv.php
      - module.audio-video.matroska.php
      - module.audio-video.quicktime.php
      - module.audio-video.riff.php
      - module.audio.ac3.php
      - module.audio.dts.php
      - module.audio.flac.php
      - module.audio.mp3.php
      - module.audio.ogg.php
      - module.tag.apetag.php
      - module.tag.id3v1.php
      - module.tag.id3v2.php
      - module.tag.lyrics3.php

- readme.txt
- images
- IXR
  - class-IXR-base64.php
  - class-IXR-client.php
  - class-IXR-clientmulticall.php
  - class-IXR-date.php
  - class-IXR-error.php
  - class-IXR-introspectionserver.php
  - class-IXR-message.php
  - class-IXR-request.php
  - class-IXR-server.php
  - class-IXR-value.php
- js
- pomo
- random_compat
- Requests
- rest-api
- SimplePie
- Text
  - Diff
  - Diff.php
- theme-compat
- widgets
- admin-bar.php
- atomlib.php
- author-template.php
- blocks.php
- bookmark-template.php
- bookmark.php
- cache.php
- canonical.php
- capabilities.php
- category-template.php
- category.php
- class-feed.php
- class-http.php
- class-IXR.php
- class-json.php
- class-oembed.php
- class-phpass.php
- class-phpmailer.php
- class-pop3.php
- class-requests.php
- class-simplepie.php
- class-smtp.php
- class-snoopy.php
- class-walker-category-dropdown.php
- class-walker-category.php

class-walker-comment.php
class-walker-nav-menu.php
class-walker-page-dropdown.php
class-walker-page.php
class-wp-admin-bar.php
class-wp-ajax-response.php
class-wp-block-parser.php
class-wp-block-type-registry.php
class-wp-block-type.php
class-wp-comment-query.php
class-wp-comment.php
class-wp-customize-control.php
class-wp-customize-manager.php
class-wp-customize-nav-menus.php
class-wp-customize-panel.php
class-wp-customize-section.php
class-wp-customize-setting.php
class-wp-customize-widgets.php
class-wp-dependency.php
class-wp-editor.php
class-wp-embed.php
class-wp-error.php
class-wp-feed-cache-transient.php
class-wp-feed-cache.php
class-wp-hook.php
class-wp-http-cookie.php
class-wp-http-curl.php
class-wp-http-encoding.php
class-wp-http-ixr-client.php
class-wp-http-proxy.php
class-wp-http-requests-hooks.php
class-wp-http-requests-response.php
class-wp-http-response.php
class-wp-http-streams.php
class-wp-image-editor-gd.php
class-wp-image-editor-imagick.php
class-wp-image-editor.php
class-wp-list-util.php
class-wp-locale-switcher.php
class-wp-locale.php
class-wp-matchesmapregex.php
class-wp-meta-query.php
class-wp-metadata-lazyloader.php
class-wp-network-query.php
class-wp-network.php
class-wp-oembed-controller.php
class-wp-post-type.php
class-wp-post.php
class-wp-query.php

class-wp-rewrite.php
class-wp-role.php
class-wp-roles.php
class-wp-session-tokens.php
class-wp-simplepie-file.php
class-wp-simplepie-sanitize-kses.php
class-wp-site-query.php
class-wp-site.php
class-wp-tax-query.php
class-wp-taxonomy.php
class-wp-term-query.php
class-wp-term.php
class-wp-text-diff-renderer-inline.php
class-wp-text-diff-renderer-table.php
class-wp-theme.php
class-wp-user-meta-session-tokens.php
class-wp-user-query.php
class-wp-user.php
class-wp-walker.php
class-wp-widget-factory.php
class-wp-widget.php
class-wp-xmlrpc-server.php
class-wp.php
class.wp-dependencies.php
class.wp-scripts.php
class.wp-styles.php
comment-template.php
comment.php
compat.php
cron.php
date.php
default-constants.php
default-filters.php
default-widgets.php
deprecated.php
embed-template.php
embed.php
feed-atom-comments.php
feed-atom.php
feed-rdf.php
feed-rss.php
feed-rss2-comments.php
feed-rss2.php
feed.php
formatting.php
functions.php
functions.wp-scripts.php
functions.wp-styles.php
general-template.php

- http.php
- kses.php
- l10n.php
- link-template.php
- load.php
- locale.php
- media-template.php
- media.php
- meta.php
- ms-blogs.php
- ms-default-constants.php
- ms-default-filters.php
- ms-deprecated.php
- ms-files.php
- ms-functions.php
- ms-load.php
- ms-network.php
- ms-settings.php
- ms-site.php
- nav-menu-template.php
- nav-menu.php
- option.php
- pluggable-deprecated.php
- pluggable.php
- plugin.php
- post-formats.php
- post-template.php

- index.php
  - #fragments
    - content

- license.txt
- readme.html
- wp-login.php
- xmlrpc.php