

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://192.168.1.2/
Scan Type	Full Scan
Start Time	Oct 25, 2025, 7:28:49 AM GMT
Scan Duration	1 hour, 40 minutes
Requests	106574
Average Response Time	1ms
Maximum Response Time	75906ms
Application Build	v24.6.240626115
Authentication Profile	-

Compliance at a Glance

CATEGORY

- 41** A01 Broken Access Control
- 11** A02 Cryptographic Failures
- 24** A03 Injection
- 10** A04 Insecure Design
- 14** A05 Security Misconfiguration
- 107** A06 Vulnerable and Outdated Components
- 9** A07 Identification and Authentication Failures
- 11** 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 Directory Traversal

WordPress is prone to a directory traversal vulnerability because it fails to sufficiently verify user-supplied input data. Exploiting this issue may allow an attacker to access sensitive information that could aid in further attacks. WordPress versions ranging from 3.7 and up to (and including) 5.0.3 are vulnerable.

CWE

CWE-22

CVSS2

AV:N/AC:L/Au:S/C:P/I:N/A:N/E:H/RL:U/RC:C

Access Vector	Network
Access Complexity	Low
Authentication	Single
Confidentiality	Partial
Integrity Impact	None
Availability Impact	None
Exploitability	High
Remediation Level	Unavailable
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/SI: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://192.168.1.2/secret/>

wordpress v4.9-4.9

Recommendation

Edit the source code to ensure that input is properly verified, or apply a fix when available

References

<https://blog.ripstech.com/2019/wordpress-image-remote-code-execution/>
<https://blog.ripstech.com/2019/wordpress-image-remote-code-execution/>

<http://foreversong.cn/archives/1364>

<http://foreversong.cn/archives/1364>

File Upload Functionality Detected

These pages allows visitors to upload files to the server. Various web applications allow users to upload files (such as pictures, images, sounds, ...). Uploaded files may pose a significant risk if not handled correctly. A remote attacker could send a multipart/form-data POST request with a specially-crafted filename or mime type and execute arbitrary code.

CVSS2

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

CVSS3

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

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

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

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

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

If the uploaded files are not safely checked an attacker may upload malicious files.

<http://192.168.1.2/>

Pages with file upload forms:

- <http://192.168.1.2/secret/wp-admin/themes.php>

```
Form name: <empty>
Form action: /secret/wp-admin/themes.php?page=custom-header&step=2
Form method: POST
Form file input: import [file]
```

Request

```
GET /secret/wp-admin/themes.php?page=custom-header HTTP/1.1
Referer: http://192.168.1.2/secret/wp-admin/
Cookie:
wordpress_c33487bf823480f7fd1fb9b067cc38a7=admin%7C1761551020%7CNjIkPD5r1iQZwR6VsF8E4KwWFQbnaUF9y0J1Wuoy59B%7C8fa1ec539c1d5e038e180bfead84990b1f18d50f2dc899bd129d6bf1007ea5d; wordpress_test_cookie=WP+Cookie+check;
wordpress_logged_in_c33487bf823480f7fd1fb9b067cc38a7=admin%7C1761551020%7CNjIkPD5r1iQZwR6VsF8E4KwWFQbnaUF9y0J1Wuoy59B%7Cba563bb9083ada55626321dd84846201cd97be483c5d9b064425f9380647d48; wp-settings-time-1=1761380427
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: 192.168.1.2
Connection: Keep-alive
```

Recommendation

Restrict file types accepted for upload: check the file extension and only allow certain files to be uploaded. Use a whitelist approach instead of a blacklist. Check for double extensions such as .php.png. Check for files without a filename like .htaccess (on ASP.NET, check for configuration files like web.config). Change the permissions on the upload folder so the files within it are not executable. If possible, rename the files that are uploaded.

WordPress 4.9.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 4.9.x ranging from 4.9 and up to (and including) 4.9.22 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

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

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

Authentication	None
Confidentiality	Partial
Integrity Impact	Partial
Availability Impact	None
Exploitability	High
Remediation Level	Official Fix
Report Confidence	Confirmed

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

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://192.168.1.2/secret/

wordpress v4.9-4.9

Recommendation

Update to WordPress version 4.9.23 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/>

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

WordPress through 4.9.6 allows Author users to execute arbitrary code by leveraging directory traversal in the wp-admin/post.php thumb parameter, which is passed to the PHP unlink function and can delete the wp-config.php file. This is related to missing filename validation in the wp-includes/post.php wp_delete_attachment function. The attacker must have capabilities for files and posts that are normally available only to the Author, Editor, and Administrator roles. The attack methodology is to delete wp-config.php and then launch a new installation process to increase the attacker's privileges.

CWE

CWE-22

CVSS3

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

Base Score	7.2
Attack Vector	Network
Attack Complexity	Low
Privileges Required	High
User Interaction	None
Scope	Unchanged
Confidentiality	High
Integrity Impact	High
Availability Impact	High

CVSS4

CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/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	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://192.168.1.2/secret/>

wordpress v4.9-4.9

<http://192.168.1.2/secret/>

wordpress v4.9-4.9

<http://192.168.1.2/secret/>

wordpress v4.9-4.9

<http://192.168.1.2/secret/>

wordpress v4.9-4.9

References

[CVE-2018-12895](#)

<https://nvd.nist.gov/vuln/detail/CVE-2018-12895>

Weak password

This page is using a weak password. Acunetix was able to guess the credentials required to access this page. A weak password is short, common, a system default, or something that could be rapidly guessed by executing a brute force attack using a subset of all possible passwords, such as words in the dictionary, proper names, words based on the user name or common variations on these themes.

CWE

CWE-200

CVSS2

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

CVSS3

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

CVSS4

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

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

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

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	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

An attacker may access the contents of the password-protected page.

<http://192.168.1.2/secret/wp-login.php>

Username: admin, Password: admin.

Request

```
POST /secret//wp-login.php HTTP/1.1
Content-type: application/x-www-form-urlencoded
Cookie: wordpress_test_cookie=WP+Cookie+check
Content-Length: 35
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: 192.168.1.2
Connection: Keep-alive

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

Recommendation

Enforce a strong password policy. Don't permit weak passwords or passwords based on dictionary words.

References

[Wikipedia - Password strength](#)

https://en.wikipedia.org/wiki/Password_strength

[Authentication Hacking Attacks](#)

<https://www.acunetix.com/websitetecurity/authentication/>

WordPress Exposure of Sensitive Information to an Unauthorized Actor Vulnerability

In WordPress before 4.9.9 and 5.x before 5.0.1, the user-activation page could be read by a search engine's web crawler if an unusual configuration were chosen. The search engine could then index and display a user's e-mail address and (rarely) the password that was generated by default.

CWE

CWE-200

CVSS3

CVSS:3.0/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

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	High
Integrity Impact	None
Availability Impact	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://192.168.1.2/secret/>

wordpress v4.9-4.9

<http://192.168.1.2/secret/>

wordpress v4.9-4.9

<http://192.168.1.2/secret/>

wordpress v4.9-4.9

References

[CVE-2018-20151](#)

<https://nvd.nist.gov/vuln/detail/CVE-2018-20151>

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://192.168.1.2/secret/>

List of WordPress users for {_nativeUrl}: {password: '', username: '', search: '', protocol: 'http', port: '', path: '/secret/', origin: 'http://192.168.1.2', href: 'http://192.168.1.2/secret/'; hostname: '192.168.1.2', host: '192.168.1.2', hash: ''});

['admin']

Request

```
POST /secret//wp-login.php HTTP/1.1
Content-type: application/x-www-form-urlencoded
Cookie: wordpress_test_cookie=WP+Cookie+check
Content-Length: 29
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: 192.168.1.2
Connection: Keep-alive

log=192&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
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://192.168.1.2/>

Possible sensitive directories:

- <http://192.168.1.2/secret>
- <http://192.168.1.2/secret/wp-admin/includes>
- <http://192.168.1.2/secret/wp-content/uploads>

Request

```
GET /secret/ 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: 192.168.1.2
```

Recommendation

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

References

[Web Server Security and Database Server Security](#)

<https://www.acunetix.com/websitetecurity/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://192.168.1.2/secret/>

Request

```
GET /secret/?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: 192.168.1.2
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](#)

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://192.168.1.2/>

Request

```
GET /zU2TNaqUB5 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: 192.168.1.2
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://192.168.1.2/>

Emails found:

- http://192.168.1.2/secret/license.txt
m@tidakada.com

Request

```
GET /secret/license.txt HTTP/1.1
Referer: http://192.168.1.2/secret/
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: 192.168.1.2
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

Web server default welcome page

This web server has a default welcome page. If you are not using this web server, it should be disabled because it may pose a security threat.

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

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

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

Integrity Impact	None
Availability Impact	None

Scope	Unchanged
Confidentiality	None
Integrity Impact	None
Availability Impact	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://192.168.1.2/>

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: 192.168.1.2
Connection: Keep-alive
```

Recommendation

If this server is not used, it is recommended to disable it.

References

[Web Server Default Welcome Page](#)

<https://www.thesitewizard.com/apache/change-default-page-for-domain.shtml>

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, or 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://192.168.1.2/>

Verified

List of cookies with missing, inconsistent or contradictory properties:

- http://192.168.1.2/secret/wp-login.php

Cookie was set with:

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

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".

- http://192.168.1.2/secret/wp-login.php

Cookie was set with:

Set-Cookie:

wordpress_c33487bf823480f7fd1fb9b067cc38a7=admin%7C1761551020%7CNjIkPD5r1iQZwR6VSf8E4KwWFQbnaUF9y0J1Wuoy59B%7C8fa1ec539c1d5e038e180bfead84990b1f18d50f2dc899bd129d6bf1007ea5d; path=/secret/wp-content/plugins; HttpOnly

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".

- http://192.168.1.2/secret/wp-login.php

Cookie was set with:

Set-Cookie:

wordpress_logged_in_c33487bf823480f7fd1fb9b067cc38a7=admin%7C1761551020%7CNjIkPD5r1iQZwR6VSf8E4KwWFQbnaUF9y0J1Wuoy59B%7Cba563bb9083ada55626321dd84846201cdd97be483c5d9b064425f9380647d48; path=/secret/; HttpOnly

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".

- http://192.168.1.2/secret/wp-admin/

Cookie was set with:

Set-Cookie: wp-settings-l=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/secret/

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".

- http://192.168.1.2/secret/wp-admin/

Cookie was set with:

Set-Cookie: wp-settings-time-l=1761378266; expires=Sun, 25-Oct-2026 07:44:26 GMT; Max-Age=31536000; path=/secret/

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".

- <http://192.168.1.2/secret/wp-admin/>

Cookie was set with:

```
Set-Cookie: wp-settings-time-1=1761378274; expires=Sun, 25-Oct-2026 07:44:34 GMT; Max-Age=31536000; path=/secret/
```

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".

- <http://192.168.1.2/secret/wp-admin/>

Cookie was set with:

```
Set-Cookie: wp-settings-time-1=1761378275; expires=Sun, 25-Oct-2026 07:44:35 GMT; Max-Age=31536000; path=/secret/
```

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".

- <http://192.168.1.2/secret/wp-admin/customize.php>

Cookie was set with:

```
Set-Cookie: wp-settings-1=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/secret/
```

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".

- <http://192.168.1.2/secret/wp-admin/customize.php>

Cookie was set with:

```
Set-Cookie: wp-settings-time-1=1761378285; expires=Sun, 25-Oct-2026 07:44:45 GMT; Max-Age=31536000; path=/secret/
```

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".

- <http://192.168.1.2/secret/wp-admin/>

Cookie was set with:

```
Set-Cookie: wp-settings-time-1=1761378684; expires=Sun, 25-Oct-2026 07:51:24 GMT; Max-Age=31536000; path=/secret/
```

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".

- <http://192.168.1.2/secret/wp-admin/customize.php>

Cookie was set with:

Set-Cookie: wp-settings-time-1=1761378987; expires=Sun, 25-Oct-2026 07:56:27 GMT; Max-Age=31536000; path=/secret/

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".

- <http://192.168.1.2/secret/wp-admin/customize.php>

Cookie was set with:

Set-Cookie: wp-settings-time-1=1761379321; expires=Sun, 25-Oct-2026 08:02:01 GMT; Max-Age=31536000; path=/secret/

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".

- <http://192.168.1.2/secret/wp-admin/>

Cookie was set with:

Set-Cookie: wp-settings-time-1=1761379582; expires=Sun, 25-Oct-2026 08:06:22 GMT; Max-Age=31536000; path=/secret/

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".

- <http://192.168.1.2/secret/wp-admin/>

Cookie was set with:

Set-Cookie: wp-settings-time-1=1761379696; expires=Sun, 25-Oct-2026 08:08:16 GMT; Max-Age=31536000; path=/secret/

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".

- <http://192.168.1.2/secret/wp-admin/customize.php>

Cookie was set with:

Set-Cookie: wp-settings-time-1=1761379771; expires=Sun, 25-Oct-2026 08:09:31 GMT; Max-Age=31536000; path=/secret/

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".

- <http://192.168.1.2/secret/wp-admin/edit-comments.php>

Cookie was set with:

```
Set-Cookie: wp-settings-l=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/secret/
```

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".

- <http://192.168.1.2/secret/wp-admin/edit-comments.php>

Cookie was set with:

```
Set-Cookie: wp-settings-time-l=1761379956; expires=Sun, 25-Oct-2026 08:12:36 GMT; Max-Age=31536000; path=/secret/
```

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".

- <http://192.168.1.2/secret/wp-admin/edit-comments.php>

Cookie was set with:

```
Set-Cookie: wp-settings-time-l=1761380003; expires=Sun, 25-Oct-2026 08:13:23 GMT; Max-Age=31536000; path=/secret/
```

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".

- <http://192.168.1.2/secret/wp-admin/edit-comments.php>

Cookie was set with:

```
Set-Cookie: wp-settings-time-l=1761380126; expires=Sun, 25-Oct-2026 08:15:26 GMT; Max-Age=31536000; path=/secret/
```

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".

- <http://192.168.1.2/secret/wp-admin/edit-comments.php>

Cookie was set with:

```
Set-Cookie: wp-settings-time-l=1761380151; expires=Sun, 25-Oct-2026 08:15:51 GMT; Max-Age=31536000; path=/secret/
```

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".

- <http://192.168.1.2/secret/wp-admin/edit-comments.php>

Cookie was set with:

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 /secret/wp-login.php HTTP/1.1
Referer: http://192.168.1.2/secret/readme.html
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: 192.168.1.2
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://192.168.1.2/secret/>

wordpress v4.9-4.9

References

[CVE-2022-43504](#)

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

WordPress 4.9.x Cross-Site Request Forgery

WordPress is prone to a cross-site request forgery vulnerability. Exploiting this issue may allow a remote attacker to perform certain administrative actions and gain unauthorized access to the affected application; other attacks are also possible. WordPress versions 4.9.x ranging from 4.9 and up to (and including) 4.9.9 are vulnerable.

CWE

CWE-352

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:R/S:U/C:L/I:L/A:L

Base Score	6.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	Required
Scope	Unchanged
Confidentiality	Low
Integrity Impact	Low
Availability Impact	Low

CVSS4

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

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

Impact

<http://192.168.1.2/secret/>

wordpress v4.9-4.9

Recommendation

Update to WordPress version 4.9.10 or latest

References

<https://blog.ripstech.com/2019/wordpress-csrf-to-rce/>

<https://blog.ripstech.com/2019/wordpress-csrf-to-rce/>

<https://cert.360.cn/warning/detail?id=149a32b8f582ee5e0cbd5f1c1b4a61de>

<https://cert.360.cn/warning/detail?id=149a32b8f582ee5e0cbd5f1c1b4a61de>

<https://wordpress.org/support.wordpress-version/version-4-9-10/>

<https://wordpress.org/support.wordpress-version/version-4-9-10/>

WordPress Cross-Site Request Forgery (CSRF) Vulnerability

WordPress before 5.1.1 does not properly filter comment content, leading to Remote Code Execution by unauthenticated users in a default configuration. This occurs because CSRF protection is mishandled, and because Search Engine Optimization of A elements is performed incorrectly, leading to XSS. The XSS results in administrative access, which allows arbitrary changes to .php files. This is related to wp-admin/includes/ajax-actions.php and wp-includes/comment.php.

CWE

CWE-352

CVSS3

CVSS:3.0/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://192.168.1.2/secret/>

wordpress v4.9-4.9

<http://192.168.1.2/secret/>

wordpress v4.9-4.9

<http://192.168.1.2/secret/>

wordpress v4.9-4.9

References

[CVE-2019-9787](#)

<https://nvd.nist.gov/vuln/detail/CVE-2019-9787>

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

Impact

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

<http://192.168.1.2/>

Verified

Folders with directory listing enabled:

- http://192.168.1.2/secret/wp-admin/css/
- http://192.168.1.2/secret/wp-admin/images/
- http://192.168.1.2/secret/wp-admin/includes/
- http://192.168.1.2/secret/wp-admin/js/
- http://192.168.1.2/secret/wp-includes/
- http://192.168.1.2/secret/wp-includes/js/
- http://192.168.1.2/secret/wp-includes/js/mediaelement/
- http://192.168.1.2/secret/wp-includes/js/mediaelement/lang/
- http://192.168.1.2/secret/wp-content/uploads/
- http://192.168.1.2/secret/wp-content/uploads/2025/
- http://192.168.1.2/secret/wp-includes/ID3/
- http://192.168.1.2/secret/wp-includes/IXR/
- http://192.168.1.2/secret/wp-includes/Requests/
- http://192.168.1.2/secret/wp-includes/SimplePie/
- http://192.168.1.2/secret/wp-includes/Text/
- http://192.168.1.2/secret/wp-includes/certificates/

Request

```
GET /secret/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: 192.168.1.2
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)

<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://192.168.1.2/>

Documentation files:

- <http://192.168.1.2/secret/readme.html>

File contents (first 100 characters):

```
<!DOCTYPE html>
<html>
<head>
<meta name="viewport" content="width=device-width" />
<meta http-equiv ...
```

- <http://192.168.1.2/secret/license.txt>

File contents (first 100 characters):

```
WordPress - Web publishing software
```

```
Copyright 2011-2017 by the contributors
```

```
This program is fr ...
```

- <http://192.168.1.2/secret/wp-content/plugins/akismet/readme.txt>

File contents (first 100 characters):

```
==== Akismet Anti-Spam ====
```

```
Contributors: matt, ryan, andy, mdawaffe, tellyworth, josephscott, lessblo ...
```

Request

```
GET /secret/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: 192.168.1.2
Connection: Keep-alive
```

Recommendation

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

Open Redirection

This endpoint is possibly vulnerable to URL redirection attacks.

URL redirection is sometimes used as a part of phishing attacks that confuse visitors about which web site they are visiting.

CWE

CWE-601

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

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

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

Availability Impact	None
---------------------	------

Confidentiality	Low
Integrity Impact	Low
Availability Impact	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

A remote attacker can redirect users from your website to a specified URL. This problem may assist an attacker to conduct phishing attacks, trojan distribution, spammers.

<http://192.168.1.2/secret/wp-admin/edit-tags.php>

URL encoded POST input `_wp_http_referer` was set to `\/bxss.me`

Request

```
POST /secret/wp-admin/edit-tags.php HTTP/1.1
Cookie:
wordpress_c33487bf823480f7fd1fb9b067cc38a7=admin%7C1761551020%7CNjIkPD5r1iQZwR6VSf8E4KwWF0bnaUF9y0J1Wuoy59B%7C8fa1ec539c1d5e038e180bfead84990b1f18d50f2dc8
899bd129d6bf1007ea5d; wordpress_test_cookie=WP+Cookie+check;
wordpress_logged_in_c33487bf823480f7fd1fb9b067cc38a7=admin%7C1761551020%7CNjIkPD5r1iQZwR6VSf8E4KwWFQbnaUF9y0J1Wuoy59B%7Cba563bb9083ada55626321dd84846201cd
d97be483c5d9b064425f9380647d48; wp-settings-time-1=1761380228
Content-Type: application/x-www-form-urlencoded
Content-Length: 205
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: 192.168.1.2
Connection: Keep-alive

_wp_http_referer=%5C/bxss.me&_wpnonce_add-tag=a59b06197e&action=add-tag&description=555&parent=-1&post_type=post&screen=edit-
category&slug=1&submit=Add%20New%20Category&tag-name=orrEuNx&taxonomy=category
```

Recommendation

Your script should properly sanitize user input.

References

[Unvalidated Redirects and Forwards Cheat Sheet](#)

https://cheatsheetseries.owasp.org/cheatsheets/Unvalidated_Redirects_and_Forwards_Cheat_Sheet.html

[HTTP Response Splitting, Web Cache Poisoning Attacks, and Related Topics](#)

https://packetstormsecurity.com/papers/general/whitepaper_httpproxy.pdf

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

Before WordPress 4.9.5, the redirection URL for the login page was not validated or sanitized if forced to use HTTPS.

CWE

CWE-601

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://192.168.1.2/secret/>

wordpress v4.9-4.9

<http://192.168.1.2/secret/>

wordpress v4.9-4.9

<http://192.168.1.2/secret/>

wordpress v4.9-4.9

<http://192.168.1.2/secret/>

wordpress v4.9-4.9

References

CVE-2018-10100

<https://nvd.nist.gov/vuln/detail/CVE-2018-10100>

WordPress Incorrect Authorization Vulnerability

In WordPress before 4.9.9 and 5.x before 5.0.1, authors could modify metadata to bypass intended restrictions on deleting files.

CWE

CWE-863

CVSS3

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

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

CVSS4

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

Base Score	7.1
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	Low
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://192.168.1.2/secret/>

wordpress v4.9-4.9

References

CVE-2018-20147

<https://nvd.nist.gov/vuln/detail/CVE-2018-20147>

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).

Weak password

This page is using a weak password. Acunetix was able to guess the credentials required to access this page. A weak password is short, common, a system default, or something that could be rapidly guessed by executing a brute force attack using a subset of all possible passwords, such as words in the dictionary, proper names, words based on the user name or common variations on these themes.

CWE

CWE-200

CVSS2

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

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

CVSS3

CVSS:3.0/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:N/PR:N/UI:N/VC:H/VI:N/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	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

An attacker may access the contents of the password-protected page.

<http://192.168.1.2/secret/wp-login.php>

Username: admin, Password: admin.

Request

```
POST /secret//wp-login.php HTTP/1.1
Content-type: application/x-www-form-urlencoded
Cookie: wordpress_test_cookie=WP+Cookie+check
Content-Length: 35
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: 192.168.1.2
Connection: Keep-alive

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

Recommendation

Enforce a strong password policy. Don't permit weak passwords or passwords based on dictionary words.

References

[Wikipedia - Password strength](#)

https://en.wikipedia.org/wiki/Password_strength

[Authentication Hacking Attacks](#)

<https://www.acunetix.com/websitesecurity/authentication/>

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://192.168.1.2/>

Verified

Folders with directory listing enabled:

- http://192.168.1.2/secret/wp-admin/css/
- http://192.168.1.2/secret/wp-admin/images/
- http://192.168.1.2/secret/wp-admin/includes/
- http://192.168.1.2/secret/wp-admin/js/
- http://192.168.1.2/secret/wp-includes/
- http://192.168.1.2/secret/wp-includes/js/
- http://192.168.1.2/secret/wp-includes/js/mediaelement/
- http://192.168.1.2/secret/wp-includes/js/mediaelement/lang/
- http://192.168.1.2/secret/wp-content/uploads/
- http://192.168.1.2/secret/wp-content/uploads/2025/
- http://192.168.1.2/secret/wp-includes/ID3/
- http://192.168.1.2/secret/wp-includes/IXR/
- http://192.168.1.2/secret/wp-includes/Requests/
- http://192.168.1.2/secret/wp-includes/SimplePie/
- http://192.168.1.2/secret/wp-includes/Text/
- http://192.168.1.2/secret/wp-includes/certificates/

Request

```
GET /secret/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: 192.168.1.2
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](#)

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://192.168.1.2/secret/>

List of WordPress users for `{'_nativeUrl': {'password': '', 'username': '', 'search': '', 'protocol': 'http', 'port': '', 'path': '/secret/', 'origin': 'http://192.168.1.2', 'href': 'http://192.168.1.2/secret/'}, 'hostname': '192.168.1.2', 'host': '192.168.1.2', 'hash': ''}}`:

`['admin']`

Request

```
POST /secret//wp-login.php HTTP/1.1
Content-type: application/x-www-form-urlencoded
Cookie: wordpress_test_cookie=WP+Cookie+check
Content-Length: 29
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: 192.168.1.2
Connection: Keep-alive

log=192&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.

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://192.168.1.2/

Documentation files:

- <http://192.168.1.2/secret/readme.html>

File contents (first 100 characters):

```
<!DOCTYPE html>
<html>
<head>
<meta name="viewport" content="width=device-width" />
<meta http-equiv ...
```

- <http://192.168.1.2/secret/license.txt>

File contents (first 100 characters):

```
WordPress - Web publishing software
```

```
Copyright 2011-2017 by the contributors
```

```
This program is fr ...
```

- <http://192.168.1.2/secret/wp-content/plugins/akismet/readme.txt>

File contents (first 100 characters):

```
== Akismet Anti-Spam ==
Contributors: matt, ryan, andy, mdawaffe, tellyworth, josephscott, lessblo ...
```

Request

```
GET /secret/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: 192.168.1.2
Connection: Keep-alive
```

Recommendation

Remove or restrict access to all documentation file accessible 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://192.168.1.2/>

Possible sensitive directories:

- <http://192.168.1.2/secret>
- <http://192.168.1.2/secret/wp-admin/includes>
- <http://192.168.1.2/secret/wp-content/uploads>

Request

```
GET /secret/ 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: 192.168.1.2
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
---------------	---------

CVSS3

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

Base Score	0.0
------------	-----

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
------------	-----

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

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

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://192.168.1.2/secret/>

Request

```
GET /secret/?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: 192.168.1.2
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

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

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

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

<http://192.168.1.2/>

Request

```
GET /zU2TNaqUB5 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: 192.168.1.2
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 spambots (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://192.168.1.2/>

Emails found:

- http://192.168.1.2/secret/license.txt
m@tidakada.com

Request

```
GET /secret/license.txt HTTP/1.1
Referer: http://192.168.1.2/secret/
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: 192.168.1.2
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://192.168.1.2/>

Verified

Request

```
GET / HTTP/1.1
Referer: http://192.168.1.2/
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: 192.168.1.2
Connection: Keep-alive

Recommendation

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

WordPress 4.9.x Multiple Vulnerabilities

WordPress is prone to multiple vulnerabilities, including cross-site scripting and security bypass vulnerabilities. An attacker may leverage these issues 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 bypass intended access restrictions by entering a string that can be directly derived from the user ID. WordPress version 4.9 is vulnerable.

CWE

CWE-330

CVSS2

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

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

CVSS3

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

Base Score	4.1
Attack Vector	Network
Attack Complexity	Low
Privileges Required	Low
User Interaction	Required
Scope	Changed
Confidentiality	None
Integrity Impact	Low
Availability Impact	None

CVSS4

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

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	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://192.168.1.2/secret/>

wordpress v4.9-4.9

Recommendation

Update to WordPress version 4.9.1 or latest

References

<https://hackerone.com/reports/249759>

<https://hackerone.com/reports/249759>

<https://wordpress.org/news/2017/11/wordpress-4-9-1-security-and-maintenance-release/>

<https://wordpress.org/news/2017/11/wordpress-4-9-1-security-and-maintenance-release/>

WordPress Use of Insufficiently Random Values Vulnerability

wp-admin/user-new.php in WordPress before 4.9.1 sets the newbloguser key to a string that can be directly derived from the user ID, which allows remote attackers to bypass intended access restrictions by entering this string.

CWE

CWE-330

CVSS3

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

Base Score	8.8
------------	-----

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

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://192.168.1.2/secret/>

wordpress v4.9-4.9

References

[CVE-2017-17091](#)

<https://nvd.nist.gov/vuln/detail/CVE-2017-17091>

A03 Injection

Injection flaws, such as SQL, NoSQL, OS, and LDAP injection, occur when untrusted data is sent to 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
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://192.168.1.2/secret/>

wordpress v4.9-4.9

References

CVE-2019-20041

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

WordPress 4.9.x Multiple Vulnerabilities

WordPress is prone to multiple vulnerabilities, including cross-site scripting, cross-site request forgery, open redirect, information disclosure 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, to perform certain administrative actions and gain unauthorized access to the affected application, to redirect users to arbitrary web sites and conduct phishing attacks, to obtain potentially sensitive information or to compromise the application, access or modify data or exploit vulnerabilities in the underlying database. WordPress versions 4.9.x ranging from 4.9 and up to (and including) 4.9.21 are vulnerable.

CWE

CWE-601

CVSS2

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

Access Vector	Network
Access Complexity	Low
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: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/

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://192.168.1.2/secret/>

wordpress v4.9-4.9

<http://192.168.1.2/secret/>

wordpress v4.9-4.9

<http://192.168.1.2/secret/>

[**http://192.168.1.2/secret/**](http://192.168.1.2/secret/)

wordpress v4.9-4.9

Recommendation

Update to WordPress version 4.9.22 or latest

References

<https://www.wordfence.com/blog/2022/10/patch-now-the-wordpress-6-0-3-security-update-contains-important-fixes/>
<https://www.wordfence.com/blog/2022/10/patch-now-the-wordpress-6-0-3-security-update-contains-important-fixes/>

<https://wordpress.org/support.wordpress-version/version-4-9-22/>
<https://wordpress.org/support.wordpress-version/version-4-9-22/>

<https://jvn.jp/en/jp/JVN09409909/index.html>
<https://jvn.jp/en/jp/JVN09409909/index.html>

WordPress Improper Control of Generation of Code ('Code Injection') Vulnerability

WordPress before 4.9.9 and 5.x before 5.0.1 allows remote code execution because an _wp_attached_file Post Meta entry can be changed to an arbitrary string, such as one ending with a .jpg?file.php substring. An attacker with author privileges can execute arbitrary code by uploading a crafted image containing PHP code in the Exif metadata. Exploitation can leverage CVE-2019-8943.

CWE

CWE-94

CVSS3

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

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	8.8
------------	-----

Base Score	9.3
------------	-----

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

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://192.168.1.2/secret/>

wordpress v4.9-4.9

References

[CVE-2019-8942](#)

<https://nvd.nist.gov/vuln/detail/CVE-2019-8942>

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

SQL injection vulnerability in stnl_iframe.php in the ShiftThis Newsletter (st_newsletter) plugin for WordPress allows remote attackers to execute arbitrary SQL commands via the newsletter parameter, a different vector than CVE-2008-0683.

CWE

CWE-138

CVSS2

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

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

Impact

<http://192.168.1.2/secret/>

wordpress v4.9-4.9

<http://192.168.1.2/secret/>

wordpress v4.9-4.9

<http://192.168.1.2/secret/>

wordpress v4.9-4.9

References

[CVE-2008-4625](#)

<https://nvd.nist.gov/vuln/detail/CVE-2008-4625>

Broken Link Hijacking

This web application contains resources (scripts or frames) that are loaded from a non-resolving (potentially expired) domain. An attacker can potentially register the expired domain and serve malicious HTML or JavaScript code (hijacking the resource).

CWE

CWE-610

CVSS2

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

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

CVSS3

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

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

CVSS4

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:H/VA:N/SC:L/SI:L/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	Low
Integrity Impact to the Subsequent System	Low
Availability Impact to the Subsequent System	None

Impact

An attacker can potentially register the expired domain and serve a malicious file that will be loaded in the context of your web application.

<http://192.168.1.2/secret/>

This page contains a `script` tag with the `src` attribute (`http://vtcsec/secret/wp-includes/js/jquery/jquery.js?ver=1.12.4`) pointing to the domain `vtcsec`. This domain does currently not resolve to an IP address and can potentially be taken over by an attacker.

Request

```
GET /secret/ HTTP/1.1
Referer: http://192.168.1.2/
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: 192.168.1.2
Connection: Keep-alive
```

Recommendation

Replace the scripts/frames that are loaded from non-resolving domains with new links that are pointing to valid domains.

References

[Broken Link Hijacking](#)

<https://edoverflow.com/2017/broken-link-hijacking/>

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 4.9.x Arbitrary File Deletion Vulnerability

WordPress is prone to a vulnerability that lets attackers delete arbitrary files because the application fails to properly verify user-supplied input. An attacker can exploit this vulnerability to delete arbitrary files in the context of the webserver process, rendering the website unusable, or even to execute arbitrary code on the webserver. WordPress versions 4.9.x ranging from 4.9 and up to (and including) 4.9.6 are vulnerable.

CWE

CWE-73

CVSS2

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

Access Vector	Network
Access Complexity	Low
Authentication	Single
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:L/UI:N/S:C/C:L/I:L/A:L

Base Score	7.4
Attack Vector	Network
Attack Complexity	Low
Privileges Required	Low
User Interaction	None
Scope	Changed
Confidentiality	Low
Integrity Impact	Low
Availability Impact	Low

CVSS4

CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:L/VI:L/VA:L/SC:N/SI: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	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://192.168.1.2/secret/>

wordpress v4.9-4.9

Recommendation

Update to WordPress version 4.9.7 or latest

References

<https://blog.ripstech.com/2018/wordpress-file-delete-to-code-execution/>

<https://blog.ripstech.com/2018/wordpress-file-delete-to-code-execution/>

<http://blog.vulnspy.com/2018/06/27/Wordpress-4-9-6-Arbitrary-File-Deletion-Vulnerability-Exploit/>

<http://blog.vulnspy.com/2018/06/27/Wordpress-4-9-6-Arbitrary-File-Deletion-Vulnerability-Exploit/>

<https://www.exploit-db.com/exploits/44949/>

<https://www.exploit-db.com/exploits/44949/>

<https://packetstormsecurity.com/files/148333/WordPress-4.9.6-Arbitrary-File-Deletion.html>

<https://packetstormsecurity.com/files/148333/WordPress-4.9.6-Arbitrary-File-Deletion.html>

<https://www.wordfence.com/blog/2018/07/details-of-an-additional-file-deletion-vulnerability-patched-in-wordpress-4-9-7/>

<https://www.wordfence.com/blog/2018/07/details-of-an-additional-file-deletion-vulnerability-patched-in-wordpress-4-9-7/>

<http://blog.nsfocus.net/wordpress-delete-any-file/>

<http://blog.nsfocus.net/wordpress-delete-any-file/>

<https://wordpress.org/news/2018/07/wordpress-4-9-7-security-and-maintenance-release/>

<https://wordpress.org/news/2018/07/wordpress-4-9-7-security-and-maintenance-release/>

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

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

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://192.168.1.2/secret/>

wordpress v4.9-4.9

<http://192.168.1.2/secret/>

wordpress v4.9-4.9

<http://192.168.1.2/secret/>

wordpress v4.9-4.9

References

[CVE-2020-28035](#)

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

WordPress 4.9.x Cross-Domain Flash Injection Vulnerability

WordPress is prone to a cross-domain Flash injection vulnerability. An attacker may leverage this issue 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 fool a user into inserting credentials on a fake Flash form. WordPress versions 4.9.x ranging from 4.9 and up to (and including) 4.9.1 are vulnerable.

CWE

CWE-269

CVSS2

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

Access Vector	Network
Access Complexity	Medium
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:H/PR:N/UI:R/S:C/C:L/I:L/A:N

Base Score	4.7
Attack Vector	Network
Attack Complexity	High
Privileges Required	None
User Interaction	Required
Scope	Changed
Confidentiality	Low
Integrity Impact	Low
Availability Impact	None

CVSS4

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

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

Impact

<http://192.168.1.2/secret/>

wordpress v4.9-4.9

Recommendation

Update to WordPress version 4.9.2 or latest

References

<https://opnsec.com/2017/10/cve-2016-9263-unpatched-xsf-vulnerability-in-wordpress/>

<https://opnsec.com/2017/10/flashme-wordpress-vulnerability-disclosure-cve-2016-9263/>

<https://wordpress.org/news/2018/01/wordpress-4-9-2-security-and-maintenance-release/>

<https://wordpress.org/news/2018/01/wordpress-4-9-2-security-and-maintenance-release/>

WordPress 4.9.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 4.9.x ranging from 4.9 and up to (and including) 4.9.15 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/S

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://192.168.1.2/secret/>

wordpress v4.9-4.9

<http://192.168.1.2/secret/>

wordpress v4.9-4.9

<http://192.168.1.2/secret/>

wordpress v4.9-4.9

Recommendation

Update to WordPress version 4.9.16 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-4-9-16/>
<https://wordpress.org/support.wordpress-version/version-4-9-16/>

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 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://192.168.1.2/>

Paths without CSP header:

- http://192.168.1.2/
- http://192.168.1.2/secret/
- http://192.168.1.2/secret/wp-admin/install.php

- http://192.168.1.2/secret/wp-admin/upgrade.php
- http://192.168.1.2/secret/readme.html
- http://192.168.1.2/secret/wp-login.php
- http://192.168.1.2/secret/wp-admin/images/
- http://192.168.1.2/secret/wp-admin/includes/
- http://192.168.1.2/secret/wp-admin/js/
- http://192.168.1.2/secret/wp-admin/css/
- http://192.168.1.2/secret/wp-admin/
- http://192.168.1.2/secret/wp-admin/customize.php
- http://192.168.1.2/secret/wp-content/plugins/akismet/
- http://192.168.1.2/secret/wp-includes/js/mediaelement/
- http://192.168.1.2/secret/wp-includes/js/mediaelement/lang/
- http://192.168.1.2/secret/wp-content/themes/
- http://192.168.1.2/secret/wp-content/uploads/
- http://192.168.1.2/secret/wp-includes/
- http://192.168.1.2/secret/wp-content/
- http://192.168.1.2/secret/wp-content/uploads/2025/
- http://192.168.1.2/secret/wp-includes/ID3/

Request

```
GET / HTTP/1.1
Referer: http://192.168.1.2/
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: 192.168.1.2
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

CVSS3

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

CVSS4

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

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

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

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://192.168.1.2/>

Locations without Permissions-Policy header:

- <http://192.168.1.2/>
- <http://192.168.1.2/secret/>
- <http://192.168.1.2/secret/wp-admin/install.php>
- <http://192.168.1.2/secret/wp-admin/upgrade.php>
- <http://192.168.1.2/secret/readme.html>
- <http://192.168.1.2/secret/wp-login.php>
- <http://192.168.1.2/secret/wp-admin/images/>
- <http://192.168.1.2/icons/>
- <http://192.168.1.2/secret/wp-admin/includes/>
- <http://192.168.1.2/secret/wp-admin/js/>
- <http://192.168.1.2/secret/wp-admin/css/>
- <http://192.168.1.2/secret/wp-admin/>
- <http://192.168.1.2/secret/wp-admin/customize.php>
- <http://192.168.1.2/secret/wp-content/plugins/akismet/>
- <http://192.168.1.2/secret/wp-includes/js/mediaelement/>
- <http://192.168.1.2/secret/wp-includes/js/mediaelement/lang/>
- <http://192.168.1.2/secret/wp-content/themes/>
- <http://192.168.1.2/secret/wp-content/uploads/>
- <http://192.168.1.2/secret/wp-includes/>
- <http://192.168.1.2/secret/wp-content/>
- <http://192.168.1.2/secret/wp-includes/ID3/>

Request

```
GET / HTTP/1.1
Referer: http://192.168.1.2/
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: 192.168.1.2
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 securely configured, but they must be patched and upgraded in a timely fashion.

Weak password

This page is using a weak password. Acunetix was able to guess the credentials required to access this page. A weak password is short, common, a system default, or something that could be rapidly guessed by executing a brute force attack using a subset of all possible passwords, such as words in the dictionary, proper names, words based on the user name or common variations on these themes.

CWE

CWE-200

CVSS2

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

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

CVSS3

CVSS:3.0/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:N/PR:N/UI:N/VC:H/VI:N/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	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

An attacker may access the contents of the password-protected page.

<http://192.168.1.2/secret/wp-login.php>

Username: admin, Password: admin.

Request

```
POST /secret//wp-login.php HTTP/1.1
Content-type: application/x-www-form-urlencoded
Cookie: wordpress_test_cookie=WP+Cookie+check
Content-Length: 35
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: 192.168.1.2
Connection: Keep-alive

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

Recommendation

Enforce a strong password policy. Don't permit weak passwords or passwords based on dictionary words.

References

[Wikipedia - Password strength](#)

https://en.wikipedia.org/wiki/Password_strength

[Authentication Hacking Attacks](#)

<https://www.acunetix.com/websitetecurity/authentication/>

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.

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://192.168.1.2/>**Verified**

Folders with directory listing enabled:

- <http://192.168.1.2/secret/wp-admin/css/>
- <http://192.168.1.2/secret/wp-admin/images/>
- <http://192.168.1.2/secret/wp-admin/includes/>
- <http://192.168.1.2/secret/wp-admin/js/>
- <http://192.168.1.2/secret/wp-includes/>
- <http://192.168.1.2/secret/wp-includes/js/>
- <http://192.168.1.2/secret/wp-includes/js/mediaelement/>
- <http://192.168.1.2/secret/wp-includes/js/mediaelement/lang/>
- <http://192.168.1.2/secret/wp-content/uploads/>
- <http://192.168.1.2/secret/wp-content/uploads/2025/>
- <http://192.168.1.2/secret/wp-includes/ID3/>
- <http://192.168.1.2/secret/wp-includes/IXR/>
- <http://192.168.1.2/secret/wp-includes/Requests/>
- <http://192.168.1.2/secret/wp-includes/SimplePie/>
- <http://192.168.1.2/secret/wp-includes/Text/>
- <http://192.168.1.2/secret/wp-includes/certificates/>

Request

```
GET /secret/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: 192.168.1.2
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>**Broken Link Hijacking**

This web application contains resources (scripts or frames) that are loaded from a non-resolving (potentially expired) domain. An attacker can potentially register the expired domain and serve malicious HTML or JavaScript code (hijacking the resource).

CWE

CWE-610

CVSS2

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

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

CVSS3

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

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

CVSS4

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:H/VA:N/SC:L/SI:L/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	Low
Integrity Impact to the Subsequent System	Low
Availability Impact to the Subsequent System	None

Impact

An attacker can potentially register the expired domain and serve a malicious file that will be loaded in the context of your web application.

<http://192.168.1.2/secret/>

This page contains a script tag with the `src` attribute (`http://vtcsec/secret/wp-includes/js/jquery/jquery.js?ver=1.12.4`) pointing to the domain `vtcsec`. This domain does currently not resolve to an IP address and can potentially be taken over by an attacker.

Request

```
GET /secret/ HTTP/1.1
Referer: http://192.168.1.2/
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: 192.168.1.2
Connection: Keep-alive
```

Recommendation

Replace the scripts/frames that are loaded from non-resolving domains with new links that are pointing to valid domains.

References

[Broken Link Hijacking](#)

<https://edoverflow.com/2017/broken-link-hijacking/>

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

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

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

Confidentiality	None
Integrity Impact	None
Availability Impact	None

User Interaction	Required
Scope	Unchanged
Confidentiality	None
Integrity Impact	None
Availability Impact	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://192.168.1.2/>

Verified

Cookies without HttpOnly flag set:

- http://192.168.1.2/secret/wp-login.php

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

- http://192.168.1.2/secret/wp-admin/

Set-Cookie: wp-settings-l=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/secret/

- http://192.168.1.2/secret/wp-admin/

Set-Cookie: wp-settings-time-1=1761378266; expires=Sun, 25-Oct-2026 07:44:26 GMT; Max-Age=31536000; path=/secret/

- http://192.168.1.2/secret/wp-admin/

Set-Cookie: wp-settings-time-1=1761378274; expires=Sun, 25-Oct-2026 07:44:34 GMT; Max-Age=31536000; path=/secret/

- http://192.168.1.2/secret/wp-admin/

Set-Cookie: wp-settings-time-1=1761378275; expires=Sun, 25-Oct-2026 07:44:35 GMT; Max-Age=31536000; path=/secret/

- http://192.168.1.2/secret/wp-admin/customize.php

Set-Cookie: wp-settings-l=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/secret/

- http://192.168.1.2/secret/wp-admin/customize.php

Set-Cookie: wp-settings-time-1=1761378285; expires=Sun, 25-Oct-2026 07:44:45 GMT; Max-Age=31536000; path=/secret/

- http://192.168.1.2/secret/wp-admin/

Set-Cookie: wp-settings-time-1=1761378684; expires=Sun, 25-Oct-2026 07:51:24 GMT; Max-Age=31536000; path=/secret/

- http://192.168.1.2/secret/wp-admin/customize.php

Set-Cookie: wp-settings-time-1=1761378987; expires=Sun, 25-Oct-2026 07:56:27 GMT; Max-Age=31536000; path=/secret/

- http://192.168.1.2/secret/wp-admin/customize.php

Set-Cookie: wp-settings-time-1=1761379321; expires=Sun, 25-Oct-2026 08:02:01 GMT; Max-Age=31536000; path=/secret/

- http://192.168.1.2/secret/wp-admin/

Set-Cookie: wp-settings-time-1=1761379582; expires=Sun, 25-Oct-2026 08:06:22 GMT; Max-Age=31536000; path=/secret/

- http://192.168.1.2/secret/wp-admin/

Set-Cookie: wp-settings-time-1=1761379696; expires=Sun, 25-Oct-2026 08:08:16 GMT; Max-Age=31536000; path=/secret/

- http://192.168.1.2/secret/wp-admin/customize.php

Set-Cookie: wp-settings-time-1=1761379771; expires=Sun, 25-Oct-2026 08:09:31 GMT; Max-Age=31536000; path=/secret/

- http://192.168.1.2/secret/wp-admin/edit-comments.php

Set-Cookie: wp-settings-1=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/secret/

- http://192.168.1.2/secret/wp-admin/edit-comments.php

Set-Cookie: wp-settings-time-1=1761379956; expires=Sun, 25-Oct-2026 08:12:36 GMT; Max-Age=31536000; path=/secret/

- http://192.168.1.2/secret/wp-admin/edit-comments.php

Set-Cookie: wp-settings-time-1=1761380003; expires=Sun, 25-Oct-2026 08:13:23 GMT; Max-Age=31536000; path=/secret/

- http://192.168.1.2/secret/wp-admin/edit-comments.php

Set-Cookie: wp-settings-time-1=1761380126; expires=Sun, 25-Oct-2026 08:15:26 GMT; Max-Age=31536000; path=/secret/

- http://192.168.1.2/secret/wp-admin/edit-comments.php

Set-Cookie: wp-settings-time-1=1761380151; expires=Sun, 25-Oct-2026 08:15:51 GMT; Max-Age=31536000; path=/secret/

- http://192.168.1.2/secret/wp-admin/edit-comments.php

Set-Cookie: wp-settings-time-1=1761380200; expires=Sun, 25-Oct-2026 08:16:40 GMT; Max-Age=31536000; path=/secret/

- http://192.168.1.2/secret/wp-admin/edit-tags.php

Set-Cookie: wp-settings-1=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/secret/

- http://192.168.1.2/secret/wp-admin/edit-tags.php

Set-Cookie: wp-settings-time-1=1761380220; expires=Sun, 25-Oct-2026 08:17:00 GMT; Max-Age=31536000; path=/secret/

Request

```
GET /secret/wp-login.php HTTP/1.1
Referer: http://192.168.1.2/secret/readme.html
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: 192.168.1.2
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, or 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://192.168.1.2/>

Verified

List of cookies with missing, inconsistent or contradictory properties:

- http://192.168.1.2/secret/wp-login.php

Cookie was set with:

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

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".

- http://192.168.1.2/secret/wp-login.php

Cookie was set with:

Set-Cookie:
wordpress_c33487bf823480f7fd1fb9b067cc38a7=admin%7C1761551020%7CNjIkPD5r1iQZwR6VSf8E4KwWFQbnaUF9y0J1Wuoy59B%7C8fa1ec539c1d5e038e180bfead84990b1f18d50f2dc899bd129d6bf1007ea5d; path=/secret/wp-content/plugins; HttpOnly

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".

- http://192.168.1.2/secret/wp-login.php

Cookie was set with:

Set-Cookie:
wordpress_logged_in_c33487bf823480f7fd1fb9b067cc38a7=admin%7C1761551020%7CNjIkPD5r1iQZwR6VSf8E4KwWFQbnaUF9y0J1Wuoy59B%7Cba563bb9083ada55626321dd84846201cdd97be483c5d9b064425f9380647d48; path=/secret/; HttpOnly

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".

- http://192.168.1.2/secret/wp-admin/

Cookie was set with:

Set-Cookie: wp-settings-l=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/secret/

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".

- http://192.168.1.2/secret/wp-admin/

Cookie was set with:

Set-Cookie: wp-settings-time-l=1761378266; expires=Sun, 25-Oct-2026 07:44:26 GMT; Max-Age=31536000; path=/secret/

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".

- http://192.168.1.2/secret/wp-admin/

Cookie was set with:

Set-Cookie: wp-settings-time-l=1761378274; expires=Sun, 25-Oct-2026 07:44:34 GMT; Max-Age=31536000; path=/secret/

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".

- http://192.168.1.2/secret/wp-admin/

Cookie was set with:

Set-Cookie: wp-settings-time-1=1761378275; expires=Sun, 25-Oct-2026 07:44:35 GMT; Max-Age=31536000; path=/secret/

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".

- http://192.168.1.2/secret/wp-admin/customize.php

Cookie was set with:

Set-Cookie: wp-settings-1=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/secret/

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".

- http://192.168.1.2/secret/wp-admin/customize.php

Cookie was set with:

Set-Cookie: wp-settings-time-1=1761378285; expires=Sun, 25-Oct-2026 07:44:45 GMT; Max-Age=31536000; path=/secret/

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".

- http://192.168.1.2/secret/wp-admin/

Cookie was set with:

Set-Cookie: wp-settings-time-1=1761378684; expires=Sun, 25-Oct-2026 07:51:24 GMT; Max-Age=31536000; path=/secret/

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".

- http://192.168.1.2/secret/wp-admin/customize.php

Cookie was set with:

Set-Cookie: wp-settings-time-1=1761378987; expires=Sun, 25-Oct-2026 07:56:27 GMT; Max-Age=31536000; path=/secret/

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".

- http://192.168.1.2/secret/wp-admin/customize.php

Cookie was set with:

Set-Cookie: wp-settings-time-1=1761379321; expires=Sun, 25-Oct-2026 08:02:01 GMT; Max-Age=31536000; path=/secret/

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".

- <http://192.168.1.2/secret/wp-admin/>

Cookie was set with:

Set-Cookie: wp-settings-time-1=1761379582; expires=Sun, 25-Oct-2026 08:06:22 GMT; Max-Age=31536000; path=/secret/

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".

- <http://192.168.1.2/secret/wp-admin/>

Cookie was set with:

Set-Cookie: wp-settings-time-1=1761379696; expires=Sun, 25-Oct-2026 08:08:16 GMT; Max-Age=31536000; path=/secret/

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".

- <http://192.168.1.2/secret/wp-admin/customize.php>

Cookie was set with:

Set-Cookie: wp-settings-time-1=1761379771; expires=Sun, 25-Oct-2026 08:09:31 GMT; Max-Age=31536000; path=/secret/

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".

- <http://192.168.1.2/secret/wp-admin/edit-comments.php>

Cookie was set with:

Set-Cookie: wp-settings-1=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/secret/

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".

- <http://192.168.1.2/secret/wp-admin/edit-comments.php>

Cookie was set with:

Set-Cookie: wp-settings-time-1=1761379956; expires=Sun, 25-Oct-2026 08:12:36 GMT; Max-Age=31536000; path=/secret/

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".

- <http://192.168.1.2/secret/wp-admin/edit-comments.php>

Cookie was set with:

Set-Cookie: wp-settings-time-1=1761380003; expires=Sun, 25-Oct-2026 08:13:23 GMT; Max-Age=31536000; path=/secret/

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".

- <http://192.168.1.2/secret/wp-admin/edit-comments.php>

Cookie was set with:

Set-Cookie: wp-settings-time-1=1761380126; expires=Sun, 25-Oct-2026 08:15:26 GMT; Max-Age=31536000; path=/secret/

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".

- <http://192.168.1.2/secret/wp-admin/edit-comments.php>

Cookie was set with:

Set-Cookie: wp-settings-time-1=1761380151; expires=Sun, 25-Oct-2026 08:15:51 GMT; Max-Age=31536000; path=/secret/

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".

- <http://192.168.1.2/secret/wp-admin/edit-comments.php>

Cookie was set with:

Set-Cookie: wp-settings-time-1=1761380200; expires=Sun, 25-Oct-2026 08:16:40 GMT; Max-Age=31536000; path=/secret/

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 /secret/wp-login.php HTTP/1.1
Referer: http://192.168.1.2/secret/readme.html
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: 192.168.1.2
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://192.168.1.2/secret/wp-admin/>

Request

```
GET /secret/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: 192.168.1.2
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://192.168.1.2/secret/wp-login.php>

Request

```
POST /secret/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: 192.168.1.2
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 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://192.168.1.2/>

Paths without CSP header:

- <http://192.168.1.2/>
- <http://192.168.1.2/secret/>

- http://192.168.1.2/secret/wp-admin/install.php
- http://192.168.1.2/secret/wp-admin/upgrade.php
- http://192.168.1.2/secret/readme.html
- http://192.168.1.2/secret/wp-login.php
- http://192.168.1.2/secret/wp-admin/images/
- http://192.168.1.2/secret/wp-admin/includes/
- http://192.168.1.2/secret/wp-admin/js/
- http://192.168.1.2/secret/wp-admin/css/
- http://192.168.1.2/secret/wp-admin/
- http://192.168.1.2/secret/wp-admin/customize.php
- http://192.168.1.2/secret/wp-content/plugins/akismet/
- http://192.168.1.2/secret/wp-includes/js/mediaelement/
- http://192.168.1.2/secret/wp-includes/js/mediaelement/lang/
- http://192.168.1.2/secret/wp-content/themes/
- http://192.168.1.2/secret/wp-content/uploads/
- http://192.168.1.2/secret/wp-includes/
- http://192.168.1.2/secret/wp-content/
- http://192.168.1.2/secret/wp-content/uploads/2025/
- http://192.168.1.2/secret/wp-includes/ID3/

Request

```
GET / HTTP/1.1
Referer: http://192.168.1.2/
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: 192.168.1.2
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://192.168.1.2/>

Request

```
GET /zU2TNaqUB5 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: 192.168.1.2
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

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

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

Confidentiality	None
Integrity Impact	None
Availability Impact	None

User Interaction	Required
Scope	Changed
Confidentiality	None
Integrity Impact	None
Availability Impact	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://192.168.1.2/>

Locations without Permissions-Policy header:

- http://192.168.1.2/
- http://192.168.1.2/secret/
- http://192.168.1.2/secret/wp-admin/install.php
- http://192.168.1.2/secret/wp-admin/upgrade.php
- http://192.168.1.2/secret/readme.html
- http://192.168.1.2/secret/wp-login.php
- http://192.168.1.2/secret/wp-admin/images/
- http://192.168.1.2/icons/
- http://192.168.1.2/secret/wp-admin/includes/
- http://192.168.1.2/secret/wp-admin/js/
- http://192.168.1.2/secret/wp-admin/css/
- http://192.168.1.2/secret/wp-admin/
- http://192.168.1.2/secret/wp-admin/customize.php
- http://192.168.1.2/secret/wp-content/plugins/akismet/
- http://192.168.1.2/secret/wp-includes/js/mediaelement/
- http://192.168.1.2/secret/wp-includes/js/mediaelement/lang/
- http://192.168.1.2/secret/wp-content/themes/
- http://192.168.1.2/secret/wp-content/uploads/
- http://192.168.1.2/secret/wp-includes/
- http://192.168.1.2/secret/wp-content/
- http://192.168.1.2/secret/wp-includes/ID3/

Request

```
GET / HTTP/1.1
Referer: http://192.168.1.2/
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: 192.168.1.2
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://192.168.1.2/secret/>

Pages where SRI is not implemented:

- http://192.168.1.2/secret/
Script SRC: <http://vtcsec/secret/wp-includes/js/jquery/jquery.js?ver=1.12.4>

Request

```
GET /secret/ HTTP/1.1
Referer: http://192.168.1.2/
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: 192.168.1.2
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/uxy9rx7HNQ1GYl1kPzQho1wx4JwY8wC"
crossorigin="anonymous"></script>
```

References

[Subresource Integrity](#)

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

[SRI Hash Generator](#)

<https://www.srihash.org/>

Web server default welcome page

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

No impact is associated with this vulnerability.

<http://192.168.1.2/>

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: 192.168.1.2
Connection: Keep-alive
```

Recommendation

If this server is not used, it is recommended to disable it.

References

[Web Server Default Welcome Page](#)

<https://www.thesitewizard.com/apache/change-default-page-for-domain.shtml>

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

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

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

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

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

<http://192.168.1.2/>

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: 192.168.1.2
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 4.9.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 4.9.x ranging from 4.9 and up to (and including) 4.9.16 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://192.168.1.2/secret/>

wordpress v4.9-4.9

Recommendation

Update to WordPress version 4.9.17 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-4-9-17/>

https://wordpress.org/support.wordpress-version/version-4-9-17/

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://192.168.1.2/secret/>

wordpress v4.9-4.9

References

[CVE-2020-28039](#)

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

WordPress Deserialization of Untrusted Data Vulnerability

In WordPress before 4.9.9 and 5.x before 5.0.1, contributors could conduct PHP object injection attacks via crafted metadata in a wp.getMediaItem XMLRPC call. This is caused by mishandling of serialized data at phar:// URLs in the wp_get_attachment_thumb_file function in wp-includes/post.php.

CWE

CWE-502

CVSS3

CVSS:3.0/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://192.168.1.2/secret/>

wordpress v4.9-4.9

References

[CVE-2018-20148](#)

<https://nvd.nist.gov/vuln/detail/CVE-2018-20148>

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

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	High
Integrity Impact	High
Availability Impact	High

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://192.168.1.2/secret/>

wordpress v4.9-4.9

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://192.168.1.2/secret/>

wordpress v4.9-4.9

<http://192.168.1.2/secret/>

wordpress v4.9-4.9

<http://192.168.1.2/secret/>

wordpress v4.9-4.9

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://192.168.1.2/secret/>

wordpress v4.9-4.9

<http://192.168.1.2/secret/>

wordpress v4.9-4.9

<http://192.168.1.2/secret/>

wordpress v4.9-4.9

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://192.168.1.2/secret/>

wordpress v4.9-4.9

<http://192.168.1.2/secret/>

wordpress v4.9-4.9

References

[CVE-2019-17670](#)

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

WordPress 4.9.x Arbitrary File Deletion Vulnerability

WordPress is prone to a vulnerability that lets attackers delete arbitrary files because the application fails to properly verify user-supplied input. An attacker can exploit this vulnerability to delete arbitrary files in the context of the webserver process, rendering the website unusable, or even to execute arbitrary code on the webserver. WordPress versions 4.9.x ranging from 4.9 and up to (and including) 4.9.6 are vulnerable.

CWE

CWE-73

CVSS2

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

Access Vector	Network
Access Complexity	Low
Authentication	Single
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:L/UI:N/S:C/C:L/I:L/A:L

Base Score	7.4
Attack Vector	Network
Attack Complexity	Low
Privileges Required	Low
User Interaction	None
Scope	Changed
Confidentiality	Low
Integrity Impact	Low
Availability Impact	Low

CVSS4

CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:L/VI:L/VA:L/SC:N/SI: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	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://192.168.1.2/secret/>

wordpress v4.9-4.9

Recommendation

Update to WordPress version 4.9.7 or latest

References

<https://blog.ripstech.com/2018/wordpress-file-delete-to-code-execution/>

https://blog.ripstech.com/2018/wordpress-file-delete-to-code-execution/

<http://blog.vulnspy.com/2018/06/27/Wordpress-4-9-6-Arbitrary-File-Delection-Vulnerability-Exploit/>

http://blog.vulnspy.com/2018/06/27/Wordpress-4-9-6-Arbitrary-File-Delection-Vulnerability-Exploit/

<https://www.exploit-db.com/exploits/44949/>

https://www.exploit-db.com/exploits/44949/

<https://packetstormsecurity.com/files/148333/WordPress-4.9.6-Arbitrary-File-Deletion.html>

https://packetstormsecurity.com/files/148333/WordPress-4.9.6-Arbitrary-File-Deletion.html

<https://www.wordfence.com/blog/2018/07/details-of-an-additional-file-deletion-vulnerability-patched-in-wordpress-4-9-7/>

https://www.wordfence.com/blog/2018/07/details-of-an-additional-file-deletion-vulnerability-patched-in-wordpress-4-9-7/

<http://blog.nsfocus.net/wordpress-delete-any-file/>

http://blog.nsfocus.net/wordpress-delete-any-file/

<https://wordpress.org/news/2018/07/wordpress-4-9-7-security-and-maintenance-release/>

https://wordpress.org/news/2018/07/wordpress-4-9-7-security-and-maintenance-release/

WordPress 4.9.x Cross-Domain Flash Injection Vulnerability

WordPress is prone to a cross-domain Flash injection vulnerability. An attacker may leverage this issue 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 fool a user into inserting credentials on a fake Flash form. WordPress versions 4.9.x ranging from 4.9 and up to (and including) 4.9.1 are vulnerable.

CWE

CWE-269

CVSS2

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

Access Vector	Network
Access Complexity	Medium
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:H/PR:N/UI:R/S:C/C:L/I:L/A:N

Base Score	4.7
Attack Vector	Network
Attack Complexity	High
Privileges Required	None
User Interaction	Required
Scope	Changed
Confidentiality	Low
Integrity Impact	Low
Availability Impact	None

CVSS4

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

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

Impact

<http://192.168.1.2/secret/>

wordpress v4.9-4.9

Recommendation

Update to WordPress version 4.9.2 or latest

References

<https://opnsec.com/2017/10/cve-2016-9263-unpatched-xsf-vulnerability-in-wordpress/>

https://opnsec.com/2017/10/cve-2016-9263-unpatched-xsf-vulnerability-in-wordpress/

<https://opnsec.com/2017/10/flashme-wordpress-vulnerability-disclosure-cve-2016-9263/>

https://opnsec.com/2017/10/flashme-wordpress-vulnerability-disclosure-cve-2016-9263/

<https://wordpress.org/news/2018/01/wordpress-4-9-2-security-and-maintenance-release/>

https://wordpress.org/news/2018/01/wordpress-4-9-2-security-and-maintenance-release/

WordPress 4.9.x Cross-Site Request Forgery

WordPress is prone to a cross-site request forgery vulnerability. Exploiting this issue may allow a remote attacker to perform certain administrative actions and gain unauthorized access to the affected application; other attacks are also possible. WordPress versions 4.9.x ranging from 4.9 and up to (and including) 4.9.9 are vulnerable.

CWE

CWE-352

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:R/S:U/C:L/I:L/A:L

Base Score	6.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	Required
Scope	Unchanged
Confidentiality	Low
Integrity Impact	Low
Availability Impact	Low

CVSS4

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

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

Impact

<http://192.168.1.2/secret/>

wordpress v4.9-4.9

Recommendation

Update to WordPress version 4.9.10 or latest

References

<https://blog.ripstech.com/2019/wordpress-csrf-to-rce/>

https://blog.ripstech.com/2019/wordpress-csrf-to-rce/

<https://cert.360.cn/warning/detail?id=149a32b8f582ee5e0cbd5f1c1b4a61de>

https://cert.360.cn/warning/detail?id=149a32b8f582ee5e0cbd5f1c1b4a61de

<https://wordpress.org/support.wordpress-version/version-4-9-10/>

https://wordpress.org/support.wordpress-version/version-4-9-10/

WordPress 4.9.x Denial of Service Vulnerability

WordPress is prone to a Denial of Service vulnerability which can be exploited by malicious people to cause the affected website to consume memory and CPU resources, thus denying service to legitimate users. WordPress versions 4.9.x ranging from 4.9 and up to (and including) 4.9.4 are vulnerable.

CWE

CWE-400

CVSS2

AV:N/AC:L/Au:N/C:N/I:N/A:P/E:POC/RL:U/RC:UR

CVSS3

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

CVSS4

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

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	None
Integrity Impact	None
Availability Impact	Partial
Exploitability	Proof of concept code
Remediation Level	Unavailable
Report Confidence	Uncorroborated

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

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	None
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://192.168.1.2/secret/>

wordpress v4.9-4.9

Recommendation

Evaluate and apply the suggested patch

References

<https://baraktawily.blogspot.ro/2018/02/how-to-dos-29-of-world-wide-websites.html>

https://baraktawily.blogspot.ro/2018/02/how-to-dos-29-of-world-wide-websites.html

<https://www.youtube.com/watch?v=nNDsGTalXSO>

https://www.youtube.com/watch?v=nNDsGTalXSO

<https://github.com/Quitten/WordPress/blob/master/wp-dos-patch.sh>

https://github.com/Quitten/WordPress/blob/master/wp-dos-patch.sh

<https://www.exploit-db.com/exploits/43968/>

https://www.exploit-db.com/exploits/43968/

<https://packetstormsecurity.com/files/146249/WordPress-Core-Denial-Of-Service.html>

https://packetstormsecurity.com/files/146249/WordPress-Core-Denial-Of-Service.html

<https://www.rastating.com/protecting-wordpress-against-cve-2018-6389/>

https://www.rastating.com/protecting-wordpress-against-cve-2018-6389/

WordPress 4.9.x Multiple Vulnerabilities

WordPress is prone to multiple vulnerabilities, including cross-site scripting, cross-site request forgery, open redirect, information disclosure 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, to perform certain administrative actions and gain unauthorized access to the affected application, to redirect users to arbitrary web sites and conduct phishing attacks, to obtain potentially sensitive information or to compromise the application, access or modify data or exploit vulnerabilities in the underlying database. WordPress versions 4.9.x ranging from 4.9 and up to (and including) 4.9.21 are vulnerable.

CWE

CWE-601

CVSS2

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

CVSS3

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

Access Vector	Network
Access Complexity	Low
Authentication	Single
Confidentiality	Partial
Integrity Impact	Partial
Availability Impact	Partial

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

CVSS4

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

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

Exploitability	High
Remediation Level	Official Fix
Report Confidence	Confirmed

Confidentiality	High
Integrity Impact	High
Availability Impact	High

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://192.168.1.2/secret/

wordpress v4.9-4.9

http://192.168.1.2/secret/

Recommendation

Update to WordPress version 4.9.22 or latest

References

<https://www.wordfence.com/blog/2022/10/patch-now-the-wordpress-6-0-3-security-update-contains-important-fixes/>

<https://www.wordfence.com/blog/2022/10/patch-now-the-wordpress-6-0-3-security-update-contains-important-fixes/>

<https://wordpress.org/support.wordpress-version/version-4-9-22/>

<https://wordpress.org/support.wordpress-version/version-4-9-22/>

<https://jvn.jp/en/jp/JVN09409909/index.html>

<https://jvn.jp/en/jp/JVN09409909/index.html>

WordPress 4.9.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 4.9.x ranging from 4.9 and up to (and including) 4.9.17 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://192.168.1.2/secret/>

wordpress v4.9-4.9

Recommendation

Update to WordPress version 4.9.18 or latest

References

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

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

<https://wordpress.org/support.wordpress-version/version-4-9-18/>

<https://wordpress.org/support.wordpress-version/version-4-9-18/>

WordPress 4.9.x Prototype Pollution

WordPress is prone to a prototype pollution vulnerability. Exploiting this issue could allow an attacker to inject key/value properties into JavaScript objects, potentially allowing for execution of arbitrary JavaScript in a user's session if they can trick that user into clicking a link. WordPress versions 4.9.x ranging from 4.9 and up to (and including) 4.9.19 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://192.168.1.2/secret/>

wordpress v4.9-4.9

Recommendation

Update to WordPress version 4.9.20 or latest

References

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

<https://wordpress.org/support/wordpress-version/version-4-9-20/>

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://192.168.1.2/secret/>

wordpress v4.9-4.9

References

[CVE-2019-17675](#)

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

WordPress Cross-Site Request Forgery (CSRF) Vulnerability

WordPress before 5.1.1 does not properly filter comment content, leading to Remote Code Execution by unauthenticated users in a default configuration. This occurs because CSRF protection is mishandled, and because Search Engine Optimization of A elements is performed incorrectly, leading to XSS. The XSS results in administrative access, which allows arbitrary changes to .php files. This is related to wp-admin/includes/ajax-actions.php and wp-includes/comment.php.

CWE

CWE-352

CVSS3

CVSS:3.0/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://192.168.1.2/secret/>

wordpress v4.9-4.9

<http://192.168.1.2/secret/>

wordpress v4.9-4.9

<http://192.168.1.2/secret/>

wordpress v4.9-4.9

References

[CVE-2019-9787](#)

<https://nvd.nist.gov/vuln/detail/CVE-2019-9787>

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

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

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://192.168.1.2/secret/>

wordpress v4.9-4.9

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://192.168.1.2/secret/>

wordpress v4.9-4.9

References

[CVE-2020-28033](#)

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

WordPress Directory Traversal

WordPress is prone to a directory traversal vulnerability because it fails to sufficiently verify user-supplied input data. Exploiting this issue may allow an attacker to access sensitive information that could aid in further attacks. WordPress versions ranging from 3.7 and up to (and including) 5.0.3 are vulnerable.

CWE

CWE-22

CVSS2

AV:N/AC:L/Au:S/C:P/I:N/A:N/E:H/RL:U/RC:C

Access Vector	Network
Access Complexity	Low
Authentication	Single
Confidentiality	Partial
Integrity Impact	None
Availability Impact	None
Exploitability	High
Remediation Level	Unavailable
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/SI: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://192.168.1.2/secret/>

wordpress v4.9-4.9

Recommendation

Edit the source code to ensure that input is properly verified, or apply a fix when available

References

<https://blog.ripstech.com/2019/wordpress-image-remote-code-execution/>
<https://blog.ripstech.com/2019/wordpress-image-remote-code-execution/>

<http://foreversong.cn/archives/1364>
<http://foreversong.cn/archives/1364>

WordPress Exposure of Sensitive Information to an Unauthorized Actor Vulnerability

In WordPress before 4.9.9 and 5.x before 5.0.1, the user-activation page could be read by a search engine's web crawler if an unusual configuration were chosen. The search engine could then index and display a user's e-mail address and (rarely) the password that was generated by default.

CWE

CWE-200

CVSS3

CVSS:3.0/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

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	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://192.168.1.2/secret/>

wordpress v4.9-4.9

<http://192.168.1.2/secret/>

wordpress v4.9-4.9

<http://192.168.1.2/secret/>

wordpress v4.9-4.9

References

[CVE-2018-20151](#)

<https://nvd.nist.gov/vuln/detail/CVE-2018-20151>

WordPress Improper Control of Generation of Code ('Code Injection') Vulnerability

WordPress before 4.9.9 and 5.x before 5.0.1 allows remote code execution because an _wp_attached_file Post Meta entry can be changed to an arbitrary string, such as one ending with a .jpg?file.php substring. An attacker with author privileges can execute arbitrary code by uploading a crafted image containing PHP code in the Exif metadata. Exploitation can leverage CVE-2019-8943.

CWE

CWE-94

CVSS3

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

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

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://192.168.1.2/secret/>

wordpress v4.9-4.9

References

[CVE-2019-8942](#)

<https://nvd.nist.gov/vuln/detail/CVE-2019-8942>

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

WordPress through 4.9.6 allows Author users to execute arbitrary code by leveraging directory traversal in the wp-admin/post.php thumb parameter, which is passed to the PHP unlink function and can delete the wp-config.php file. This is related to missing filename validation in the wp-includes/post.php wp_delete_attachment function. The attacker must have capabilities for files and posts that are normally available only to the Author, Editor, and Administrator roles. The attack methodology is to delete wp-config.php and then launch a new installation process to increase the attacker's privileges.

CWE

CWE-22

CVSS3

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

Base Score	7.2
Attack Vector	Network
Attack Complexity	Low
Privileges Required	High
User Interaction	None
Scope	Unchanged
Confidentiality	High
Integrity Impact	High
Availability Impact	High

CVSS4

CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/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	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://192.168.1.2/secret/>

wordpress v4.9-4.9

<http://192.168.1.2/secret/>

wordpress v4.9-4.9

<http://192.168.1.2/secret/>

wordpress v4.9-4.9

<http://192.168.1.2/secret/>

wordpress v4.9-4.9

References

[CVE-2018-12895](#)

<https://nvd.nist.gov/vuln/detail/CVE-2018-12895>

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

SQL injection vulnerability in stnl_iframe.php in the ShiftThis Newsletter (st_newsletter) plugin for WordPress allows remote attackers to execute arbitrary SQL commands via the newsletter parameter, a different vector than CVE-2008-0683.

CWE

CWE-138

CVSS2

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

Access Vector	Network
Access Complexity	Low
Authentication	None

Confidentiality	Partial
Integrity Impact	Partial
Availability Impact	Partial

Impact

<http://192.168.1.2/secret/>

wordpress v4.9-4.9

<http://192.168.1.2/secret/>

wordpress v4.9-4.9

<http://192.168.1.2/secret/>

wordpress v4.9-4.9

References

[CVE-2008-4625](#)

<https://nvd.nist.gov/vuln/detail/CVE-2008-4625>

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://192.168.1.2/secret/>

wordpress v4.9-4.9

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://192.168.1.2/secret/>

wordpress v4.9-4.9

Recommendation

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

References

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

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

WordPress Uncontrolled Resource Consumption Vulnerability

In WordPress through 4.9.2, unauthenticated attackers can cause a denial of service (resource consumption) by using the large list of registered .js files (from wp-includes/script-loader.php) to construct a series of requests to load every file many times.

CWE

CWE-400

CVSS3

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

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

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
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://192.168.1.2/secret/>

wordpress v4.9-4.9

<http://192.168.1.2/secret/>

wordpress v4.9-4.9

References

CVE-2018-6389

<https://nvd.nist.gov/vuln/detail/CVE-2018-6389>

WordPress Use of Insufficiently Random Values Vulnerability

wp-admin/user-new.php in WordPress before 4.9.1 sets the newbloguser key to a string that can be directly derived from the user ID, which allows remote attackers to bypass intended access restrictions by entering this string.

CWE

CWE-330

CVSS3

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

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

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://192.168.1.2/secret/>

wordpress v4.9-4.9

References

CVE-2017-17091

<https://nvd.nist.gov/vuln/detail/CVE-2017-17091>

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://192.168.1.2/secret/>

wordpress v4.9-4.9

References

[CVE-2020-11027](#)

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

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

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://192.168.1.2/secret/>

wordpress v4.9-4.9

References

[CVE-2020-25286](#)

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://192.168.1.2/secret/>

wordpress v4.9-4.9

References

[CVE-2022-43504](https://nvd.nist.gov/vuln/detail/CVE-2022-43504)

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

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

<http://192.168.1.2/secret/>

wordpress v4.9-4.9

References

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

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
Privileges Required	Low
User Interaction	Required
Scope	Changed
Confidentiality	None
Integrity Impact	High
Availability Impact	None

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://192.168.1.2/secret/>

wordpress v4.9-4.9

<http://192.168.1.2/secret/>

wordpress v4.9-4.9

References

CVE-2020-4047

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

WordPress Incorrect Authorization Vulnerability

In WordPress before 4.9.9 and 5.x before 5.0.1, authors could modify metadata to bypass intended restrictions on deleting files.

CWE

CWE-863

CVSS3

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

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

CVSS4

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

Base Score	7.1
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	Low
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://192.168.1.2/secret/>

wordpress v4.9-4.9

References

[CVE-2018-20147](#)

<https://nvd.nist.gov/vuln/detail/CVE-2018-20147>

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://192.168.1.2/secret/>

wordpress v4.9-4.9

References

[CVE-2022-3590](#)

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

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

Before WordPress 4.9.5, the redirection URL for the login page was not validated or sanitized if forced to use HTTPS.

CWE

CWE-601

CVSS3

CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S: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://192.168.1.2/secret/>

wordpress v4.9-4.9

<http://192.168.1.2/secret/>

wordpress v4.9-4.9

<http://192.168.1.2/secret/>

wordpress v4.9-4.9

<http://192.168.1.2/secret/>

wordpress v4.9-4.9

References

CVE-2018-10100

<https://nvd.nist.gov/vuln/detail/CVE-2018-10100>

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://192.168.1.2/secret/>

wordpress v4.9-4.9

References

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://192.168.1.2/>

Verified

Request

```
GET / HTTP/1.1
Referer: http://192.168.1.2/
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: 192.168.1.2
Connection: Keep-alive
```

Recommendation

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

Weak password

This page is using a weak password. Acunetix was able to guess the credentials required to access this page. A weak password is short, common, a system default, or something that could be rapidly guessed by executing a brute force attack using a subset of all possible passwords, such as words in the dictionary, proper names, words based on the user name or common variations on these themes.

CWE

CWE-200

CVSS2

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

CVSS3

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

CVSS4

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

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

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

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	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

An attacker may access the contents of the password-protected page.

<http://192.168.1.2/secret/wp-login.php>

Username: admin, Password: admin.

Request

```
POST /secret//wp-login.php HTTP/1.1
Content-type: application/x-www-form-urlencoded
Cookie: wordpress_test_cookie=WP+Cookie+check
Content-Length: 35
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: 192.168.1.2
Connection: Keep-alive

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

Recommendation

Enforce a strong password policy. Don't permit weak passwords or passwords based on dictionary words.

References

[Wikipedia - Password strength](#)

https://en.wikipedia.org/wiki/Password_strength

[Authentication Hacking Attacks](#)

<https://www.acunetix.com/websitetecurity/authentication/>

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

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

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

Integrity Impact	None
Availability Impact	None

Confidentiality	Low
Integrity Impact	None
Availability Impact	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 enumerate the WordPress usernames and use this information to conduct brute-force attacks against passwords for these known usernames.

<http://192.168.1.2/secret/>

List of WordPress users for `{'_nativeUrl': {'password': '', 'username': '', 'search': '', 'protocol': 'http', 'port': '', 'path': '/secret/'}, 'origin': 'http://192.168.1.2', 'href': 'http://192.168.1.2/secret/'}, 'hostname': '192.168.1.2', 'host': '192.168.1.2', 'hash': ''}}`:

```
[admin]
```

Request

```
POST /secret//wp-login.php HTTP/1.1
Content-type: application/x-www-form-urlencoded
Cookie: wordpress_test_cookie=WP+Cookie+check
Content-Length: 29
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: 192.168.1.2
Connection: Keep-alive

log=192&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

Impact

No impact is associated with this vulnerability.

<http://192.168.1.2/secret/wp-login.php>

Request

```
POST /secret//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: 192.168.1.2
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://192.168.1.2/secret/wp-admin/>

Request

```
GET /secret/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: 192.168.1.2
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://192.168.1.2/secret/>

wordpress v4.9-4.9

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
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://192.168.1.2/secret/>

wordpress v4.9-4.9

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://192.168.1.2/secret/>

wordpress v4.9-4.9

References

CVE-2020-11028

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

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://192.168.1.2/secret/>

wordpress v4.9-4.9

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

In WordPress before 4.9.9 and 5.x before 5.0.1, contributors could conduct PHP object injection attacks via crafted metadata in a wp.getMediaItem XMLRPC call. This is caused by mishandling of serialized data at phar:// URLs in the wp_get_attachment_thumb_file function in wp-includes/post.php.

CWE

CWE-502

CVSS3

CVSS:3.0/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://192.168.1.2/secret/>

wordpress v4.9-4.9

References

[CVE-2018-20148](#)

<https://nvd.nist.gov/vuln/detail/CVE-2018-20148>

WordPress 4.9.x Multiple Vulnerabilities

WordPress is prone to multiple vulnerabilities, including deserialization and PHP file upload vulnerabilities. Exploiting these issues could allow an attacker to call arbitrary PHP Objects that can be used to perform a variety of malicious actions, granted a POP chain is also present or to upload arbitrary code and run it in the context of the webserver process, which may facilitate unauthorized access or privilege escalation. WordPress versions 4.9.x ranging from 4.9 and up to (and including) 4.9.24 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

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

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

Confidentiality	Partial
Integrity Impact	Partial
Availability Impact	Partial
Exploitability	High
Remediation Level	Official Fix
Report Confidence	Confirmed

Privileges Required	High
User Interaction	None
Scope	Changed
Confidentiality	High
Integrity Impact	High
Availability Impact	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://192.168.1.2/secret/>

wordpress v4.9-4.9

<http://192.168.1.2/secret/>

wordpress v4.9-4.9

<http://192.168.1.2/secret/>

wordpress v4.9-4.9

<http://192.168.1.2/secret/>

wordpress v4.9-4.9

Recommendation

Update to WordPress version 4.9.25 or latest

References

<https://wordpress.org/news/2024/01/wordpress-6-4-3-maintenance-and-security-release/>

https://wordpress.org/news/2024/01/wordpress-6-4-3-maintenance-and-security-release/

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

CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/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

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

Availability Impact	None
---------------------	------

Integrity Impact	None
Availability Impact	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://192.168.1.2/secret/>

Pages where SRI is not implemented:

- http://192.168.1.2/secret/
- Script SRC: <http://vtcsec/secret/wp-includes/js/jquery/jquery.js?ver=1.12.4>

Request

```
GET /secret/ HTTP/1.1
Referer: http://192.168.1.2/
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: 192.168.1.2
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-oqVuAfXKap7fdgcCY5uykM6+R9GqQ8K/uxy9rx7HNQ1GYl1kPzQho1wx4JwY8wC"
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 4.9.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 4.9.x ranging from 4.9 and up to (and including) 4.9.17 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

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

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

Exploitability	Proof of concept code
Remediation Level	Official Fix
Report Confidence	Confirmed

Confidentiality	High
Integrity Impact	High
Availability Impact	High

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://192.168.1.2/secret/>

wordpress v4.9-4.9

Recommendation

Update to WordPress version 4.9.18 or latest

References

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

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

<https://wordpress.org/support.wordpress-version/version-4-9-18/>

https://wordpress.org/support.wordpress-version/version-4-9-18/

A09 Security Logging and Monitoring Failures

Insufficient logging and monitoring, coupled with missing or ineffective integration with incident response, allows attackers to further attack systems, 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

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://192.168.1.2/secret/

wordpress v4.9-4.9

http://192.168.1.2/secret/

wordpress v4.9-4.9

References

[CVE-2019-17670](#)

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

WordPress 4.9.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 4.9.x ranging from 4.9 and up to (and including) 4.9.11 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://192.168.1.2/secret/

wordpress v4.9-4.9

Recommendation

Update to WordPress version 4.9.12 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-4-9-12/>

<https://wordpress.org/support.wordpress-version/version-4-9-12/>

<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
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://192.168.1.2/secret/>

wordpress v4.9-4.9

Recommendation

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

References

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

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

<https://sploit.us/exploit?id=WPEX-ID:C8814E6E-78B3-4F63-A1D3-6906A84C1F11>

<https://sploit.us/exploit?id=WPEX-ID:C8814E6E-78B3-4F63-A1D3-6906A84C1F11>

Coverage

http://192.168.1.2

- icons
- secret
 - #fragments
 - content
- wp-admin
 - #fragments
 - comments-form
 - tab-panel-help-content
 - tab-panel-help-layout
 - tab-panel-help-navigation
 - tab-panel-overview
 - wp-toolbar
 - wpbody-content
- css
 - install.css
- images
- includes
- js
- user
 - async-upload.php
 - comment.php
 - customize.php
 - edit-comments.php
 - #fragments
 - comments-form
 - tab-panel-moderating-comments
 - tab-panel-overview
 - wp-toolbar
 - wpbody-content
 - edit-tags.php
 - #fragments
 - tab-panel-adding-terms
 - tab-panel-overview
 - wp-toolbar
 - wpbody-content
 - edit.php
 - #fragments
 - tab-panel-action-links
 - tab-panel-bulk-actions
 - tab-panel-overview
 - tab-panel-screen-content
 - wp-toolbar
 - wpbody-content
 - export.php
 - import.php
 - index.php

```
install.php  
media-new.php  
nav-menus.php  
options-discussion.php  
options-general.php  
options-media.php  
options-permalink.php  
options-reading.php  
options-writing.php  
plugin-editor.php  
plugin-install.php  
plugins.php  
post-new.php  
#fragments  
comments-form  
edit_timestamp  
post_status  
tab-panel-about-pages  
tab-panel-inserting-media  
tab-panel-page-attributes  
visibility  
wp-toolbar  
wpbody-content  
post.php  
profile.php  
theme-editor.php  
themes.php  
#fragments  
tab-panel-overview  
tab-panel-set-header-image  
tab-panel-set-header-text  
wp-toolbar  
wpbody-content  
tools.php  
update-core.php  
upgrade.php  
upload.php  
user-new.php  
users.php  
widgets.php  
wp-content  
plugins  
akismet  
readme.txt  
themes  
uploads  
2025  
wp-includes  
certificates
```

- css
- customize
- fonts
- ID3
- 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

- mediaelement
 - lang
 - renderers
 - mediaelement-and-player.js
 - mediaelement-and-player.min.js
 - mediaelement-flash-audio-ogg.swf
 - mediaelement-flash-audio.swf
 - mediaelement-flash-video-hls.swf
 - mediaelement-flash-video-mdash.swf
 - mediaelement-flash-video.swf
 - mediaelement-migrate.js
 - mediaelement-migrate.min.js
 - mediaelement.js
 - mediaelement.min.js
 - mediaelementplayer-legacy.css
 - mediaelementplayer-legacy.min.css
 - mediaelementplayer.css
 - mediaelementplayer.min.css
 - wp-mediaelement.css
 - wp-mediaelement.js
 - wp-mediaelement.min.css
 - wp-mediaelement.min.js
 - wp-playlist.js
 - wp-playlist.min.js

- pomo

- random_compat
- Requests
- rest-api
- SimplePie
- Text
 - Diff
 - Diff.php

-  theme-compat
-  widgets
-  admin-bar.php
-  atomlib.php
-  author-template.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-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-settings.php
- nav-menu-template.php
- nav-menu.php
- option.php
- pluggable-deprecated.php
- pluggable.php
- plugin.php
- post-formats.php
- post-template.php
- post-thumbnail-template.php

 post.php
 query.php
 registration-functions.php
 registration.php
 rest-api.php

 license.txt

 readme.html

 wp-login.php