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://192.168.1.5/
Scan Type	Full Scan
Start Time	Nov 3, 2025, 9:10:15 AM GMT
Scan Duration	43 minutes
Requests	35227
Average Response Time	1ms
Maximum Response Time	85480ms
Application Build	v24.6.240626115
Authentication Profile	-

Compliance at a Glance

CATEGORY	
21	A01 Broken Access Control
9	A02 Cryptographic Failures
19	A03 Injection
5	A04 Insecure Design
8	A05 Security Misconfiguration
67	A06 Vulnerable and Outdated Components
5	A07 Identification and Authentication Failures
4	A08 Software and Data Integrity Failures
0	A09 Security Logging and Monitoring Failures
1	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.

ReFlex Gallery Arbitrary File Upload

WordPress Plugin ReFlex Gallery is prone to a vulnerability that lets attackers upload arbitrary files because the application fails to properly sanitize user-supplied input. An attacker can exploit this vulnerability to upload arbitrary code and run it in the context of the webserver process. This may facilitate unauthorized access or privilege escalation; other attacks are also possible. WordPress Plugin ReFlex Gallery version 3.1.3 is vulnerable; prior versions may also be affected.

CWE
CWE-434

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

Access Vector	Network
Access Complexity	Low
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:C/C:L/I:L/A:L

Base Score	8.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Changed
Confidentiality	Low
Integrity Impact	Low
Availability Impact	Low

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

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

Impact

http://192.168.1.5/wordpress/wp-content/plugins/reflex-gallery/

reflex-gallery v3.1.3-3.1.3

Recommendation

Update to plugin version 3.1.4 or latest

References

http://www.exploit-db.com/exploits/36374/
http://www.exploit-db.com/exploits/36374/

http://packetstormsecurity.com/files/130845/WordPress-Reflex-Gallery-3.1.3-Shell-Upload.html
http://packetstormsecurity.com/files/130845/WordPress-Reflex-Gallery-3.1.3-Shell-Upload.html

https://github.com/googleinurl/Wordpress-Plugin-Reflex-Gallery-Arbitrary-File-Upload
https://github.com/googleinurl/Wordpress-Plugin-Reflex-Gallery-Arbitrary-File-Upload

http://packetstormsecurity.com/files/131515/WordPress-Reflex-Gallery-Upload.html
http://packetstormsecurity.com/files/131515/WordPress-Reflex-Gallery-Upload.html

https://www.exploit-db.com/exploits/36809/
https://www.exploit-db.com/exploits/36809/

Shopping Cart & eCommerce Store Arbitrary File Upload

WordPress Plugin Shopping Cart & eCommerce Store is prone to a vulnerability that lets attackers upload arbitrary files because the application fails to properly sanitize user-supplied input. An attacker can exploit this vulnerability to upload arbitrary code and run it in the context of the webserver process. This may facilitate unauthorized access or privilege escalation; other attacks are also possible. WordPress Plugin Shopping Cart & eCommerce Store version 3.0.8 is vulnerable; prior versions may also be affected.

CWE
CWE-434

CVSS2
AV:N/AC:L/Au:S/C:C/I:C/A:N/E:F/RL:OF/RC:C

Access Vector	Network
Access Complexity	Low
Authentication	Single
Confidentiality	Complete
Integrity Impact	Complete
Availability Impact	None
Exploitability	Functional exploit exists
Remediation Level	Official Fix
Report Confidence	Confirmed

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

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

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

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

Impact

http://192.168.1.5/wordpress/wp-content/plugins/wp-easycart/

wp-easycart v3.0.4-3.0.4

Recommendation

Update to plugin version 3.0.9 or latest

References

http://security.szurek.pl/wordpress-shopping-cart-304-unrestricted-file-upload.html
http://security.szurek.pl/wordpress-shopping-cart-304-unrestricted-file-upload.html

http://www.exploit-db.com/exploits/35730/
http://www.exploit-db.com/exploits/35730/

http://packetstormsecurity.com/files/129875/WordPress-Shopping-Cart-3.0.4-Unrestricted-File-Upload.html
http://packetstormsecurity.com/files/129875/WordPress-Shopping-Cart-3.0.4-Unrestricted-File-Upload.html

http://www.exploit-db.com/exploits/36043/
http://www.exploit-db.com/exploits/36043/

http://packetstormsecurity.com/files/130328/WordPress-WP-EasyCart-Unrestricted-File-Upload.html
http://packetstormsecurity.com/files/130328/WordPress-WP-EasyCart-Unrestricted-File-Upload.html

Slideshow Gallery LITE Arbitrary File Upload

WordPress Plugin Slideshow Gallery LITE is prone to a vulnerability that lets attackers upload arbitrary files. The issue occurs because the application fails to adequately sanitize user-supplied input. An attacker can exploit this vulnerability to upload arbitrary code and run it in the context of the webserver process. This may facilitate unauthorized access or privilege escalation; other attacks are also possible. WordPress Plugin Slideshow Gallery LITE version 1.4.6 is vulnerable; prior versions may also be affected.

CWE
CWE-20

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

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

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

Access Vector	Network
Access Complexity	Low
Authentication	Single
Confidentiality	Partial
Integrity Impact	Partial
Availability Impact	Partial
Exploitability	Functional exploit exists
Remediation Level	Official Fix
Report Confidence	Confirmed

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

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://192.168.1.5/wordpress/wp-content/plugins/slideshow-gallery/

slideshow-gallery v1.4.6-1.4.6

Recommendation

Update to plugin version 1.4.7 or latest

References

http://whitexploit.blogspot.mx/2014/08/wordpress-slideshow-gallery-146-shell.html
http://whitexploit.blogspot.mx/2014/08/wordpress-slideshow-gallery-146-shell.html

http://www.exploit-db.com/exploits/34514/
http://www.exploit-db.com/exploits/34514/

http://www.exploit-db.com/exploits/34681/
http://www.exploit-db.com/exploits/34681/

http://packetstormsecurity.com/files/128069/WordPress-Slideshow-Gallery-1.4.6-Shell-Upload.html
http://packetstormsecurity.com/files/128069/WordPress-Slideshow-Gallery-1.4.6-Shell-Upload.html

http://packetstormsecurity.com/files/131526/WordPress-SlideShow-Gallery-Authenticated-File-Upload.html
http://packetstormsecurity.com/files/131526/WordPress-SlideShow-Gallery-Authenticated-File-Upload.html

http://secunia.com/advisories/60074/
http://secunia.com/advisories/60074/

WordPress XML-RPC authentication brute force

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

CWE

CWE-521

CVSS2

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

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

CVSS3

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

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

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	None

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

Impact

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

http://192.168.1.5/wordpress/xmlrpc.php

Pattern found:

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

Request

```
POST /wordpress//xmlrpc.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Cookie: ec_cart_id=GBBQYPNKBUSYMSPGDLURKTQEGRKPQF; PHPSESSID=nt36t21i6j2s3qvn17255ejgni
Content-Length: 264
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0 Safari/537.36
Host: 192.168.1.5
Connection: Keep-alive

<?xml version="1.0" encoding="iso-8859-1"?>
<methodCall>
<methodName>wp.getUsersBlogs</methodName>
<params>
<param><value><string>admin</string></value></param>
<param><value><string>894758954378954375349 87</string></value>
</param>
</params>
</methodCall>
```

Recommendation

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

References

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

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

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

Shopping Cart & eCommerce Store Multiple Security Bypass Vulnerabilities

WordPress Plugin Shopping Cart & eCommerce Store is prone to multiple security bypass vulnerabilities. Exploiting these issues may allow attackers to perform otherwise restricted actions and subsequently update any WordPress options. WordPress Plugin Shopping Cart & eCommerce Store version 3.0.20 is vulnerable; prior versions may also be affected.

CWE

CWE-264

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

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

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

Integrity Impact	Partial
Availability Impact	Partial
Exploitability	Proof of concept code
Remediation Level	Official Fix
Report Confidence	Confirmed

User Interaction	None
Scope	Changed
Confidentiality	Low
Integrity Impact	Low
Availability Impact	Low

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://192.168.1.5/wordpress/wp-content/plugins/wp-easycart/

wp-easycart v3.0.4-3.0.4

Recommendation

Update to plugin version 3.0.22 or latest

References

https://www.rastating.com/wp-easycart-privilege-escalation-information-disclosure/
https://www.rastating.com/wp-easycart-privilege-escalation-information-disclosure/

https://github.com/rapid7/metasploit-framework/blob/master/modules/auxiliary/admin/http/wp_easycart_privilege_escalation.rb
https://github.com/rapid7/metasploit-framework/blob/master/modules/auxiliary/admin/http/wp_easycart_privilege_escalation.rb

WP Support Plus Responsive Ticket System Security Bypass

WordPress Plugin WP Support Plus Responsive Ticket System is prone to a security bypass vulnerability. Exploiting this issue may allow attackers to perform otherwise restricted actions and subsequently login as any user without knowing the password. WordPress Plugin WP Support Plus Responsive Ticket System version 7.1.4 is vulnerable; prior versions may also be affected.

CWE
CWE-287

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

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

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

Base Score	7.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity Impact	Low
Availability Impact	Low

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

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

Impact

http://192.168.1.5/wordpress/wp-content/plugins/wp-support-plus-responsive-ticket-system/

wp-support-plus-responsive-ticket-system v7.1.3-7.1.3

Recommendation

Update to plugin version 8.0.0 or latest

References

https://security.szurek.pl/wp-support-plus-responsive-ticket-system-713-privilege-escalation.html
https://security.szurek.pl/wp-support-plus-responsive-ticket-system-713-privilege-escalation.html

https://plugins.svn.wordpress.org/wp-support-plus-responsive-ticket-system/trunk/readme.txt
https://plugins.svn.wordpress.org/wp-support-plus-responsive-ticket-system/trunk/readme.txt

Mail Masta Local File Inclusion

WordPress Plugin Mail Masta is prone to a local file inclusion vulnerability because it fails to sufficiently verify user-supplied input. Exploiting this issue may allow an attacker to obtain sensitive information that could aid in further attacks. WordPress Plugin Mail Masta version 1.0 is vulnerable.

CWE
CWE-22

CVSS2
AV:N/AC:L/Au:N/C:P/I:N/A:N/E:POC/RL:U/RC:UR

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

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

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

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

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

http://192.168.1.5/wordpress/wp-content/plugins/mail-masta/

mail-masta v1.0-1.0

Recommendation

Edit the source code to ensure that input is properly verified or disable the plugin until a fix is available

References

https://www.exploit-db.com/exploits/40290/
https://www.exploit-db.com/exploits/40290/

https://packetstormsecurity.com/files/138481/WordPress-Mail-Master-1.0-Local-File-Inclusion.html
https://packetstormsecurity.com/files/138481/WordPress-Mail-Master-1.0-Local-File-Inclusion.html

Site Editor-WordPress Site Builder-Theme Builder and Page Builder Local File Inclusion

WordPress Plugin Site Editor-WordPress Site Builder-Theme Builder and Page Builder is prone to a local file inclusion vulnerability because it fails to sufficiently verify user-supplied input. Exploiting this issue may allow an attacker to obtain sensitive information that could aid in further attacks. WordPress Plugin Site Editor-WordPress Site Builder-Theme Builder and Page Builder version 1.1.1 is vulnerable; prior versions may also be affected.

CWE
CWE-22

CVSS2
AV:N/AC:L/Au:N/C:P/I:N/A:N/E:POC/RL:U/RC:C

Access Vector	Network

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

Base Score	5.8

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

Base Score	6.9

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

Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Changed
Confidentiality	Low
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	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://192.168.1.5/wordpress/wp-content/plugins/site-editor/

site-editor v1.1.1-1.1.1

Recommendation

Edit the source code to ensure that input is properly verified or disable the plugin until a fix is available

References

http://seclists.org/fulldisclosure/2018/Mar/40
http://seclists.org/fulldisclosure/2018/Mar/40

https://www.exploit-db.com/exploits/44340/
https://www.exploit-db.com/exploits/44340/

https://packetstormsecurity.com/files/146796/WordPress-Site-Editor-1.1.1-Local-File-Inclusion.html
https://packetstormsecurity.com/files/146796/WordPress-Site-Editor-1.1.1-Local-File-Inclusion.html

Slideshow Gallery LITE Multiple Vulnerabilities

WordPress Plugin Slideshow Gallery LITE is prone to multiple vulnerabilities, including cross-site scripting and information disclosure vulnerabilities. Exploiting these issues could allow an attacker to execute arbitrary script code in the browser of an unsuspecting user in the context of the affected site, allowing the attacker to steal cookie-based authentication credentials or to obtain sensitive information which may help in launching further attacks. WordPress Plugin Slideshow Gallery LITE version 1.5.1 is vulnerable; prior versions may also be affected.

CWE
CWE-200

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

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

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:P/PR:N/UI:N/VC:H/VI:N/VA:N/SC: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://192.168.1.5/wordpress/wp-content/plugins/slideshow-gallery/

slideshow-gallery v1.4.6-1.4.6

Recommendation

Update to plugin version 1.5.2 or latest

References

http://zwx.fr/advisories/2014/Wordpress%20Plugin%20Slideshow%20Gallery%201.5.1%20-%20Multiple%20Vulnerability.txt
http://zwx.fr/advisories/2014/Wordpress%20Plugin%20Slideshow%20Gallery%201.5.1%20-%20Multiple%20Vulnerability.txt

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://192.168.1.5/wordpress/

List of WordPress users for {'_nativeUrl': {'password': '', 'username': '', 'search': '', 'protocol': 'http', 'port': '', 'path': '/wordpress/', 'origin': 'http://192.168.1.5', 'href': 'http://192.168.1.5/wordpress/', 'hostname': '192.168.1.5', 'host': '192.168.1.5', 'hash': ''}}:

['admin']

Request

```
POST /wordpress//wp-login.php HTTP/1.1
Content-type: application/x-www-form-urlencoded
Cookie: comment_author_311f7ebdbf2fdff1bfa4c4b8376b4bbf=sOdPqaAH; comment_author_email_311f7ebdbf2fdff1bfa4c4b8376b4bbf=testing%40example.com;
comment_author_url_311f7ebdbf2fdff1bfa4c4b8376b4bbf=http%3A%2F%2Fwww.example.com; ec_cart_id=KRZULVEOJJCQRXPJOVCUNFMMHEFDBE;
PHPSESSID=aqceka9dkvqmo63rrm46ru828b
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: 192.168.1.5
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://192.168.1.5/

Possible sensitive directories:

- http://192.168.1.5/wordpress/wp-content/**uploads**
- http://192.168.1.5/wordpress/wp-content/plugins/site-editor/**includes**
- http://192.168.1.5/wordpress/wp-content/plugins/site-editor/editor/**includes**
- http://192.168.1.5/wordpress/wp-content/plugins/site-editor/editor/extensions/pagebuilder/**includes**

Request

```
GET /wordpress/wp-content/uploads/ HTTP/1.1
Cookie: ec_cart_id=GBBQYPNKBUSYMSPGDLURKTQEGRKPQF; PHPSESSID=nt36t21i6j2s3qvn17255ejgni
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: 192.168.1.5
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/

[Possible] Internal Path Disclosure (*nix)

One or more fully qualified path names were found. From this information the attacker may learn the file system structure from the web server. This information can be used to conduct further attacks.

This alert may be a false positive, manual confirmation is required.

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

Possible sensitive information disclosure.

http://192.168.1.5/

Pages with paths being disclosed:

- http://192.168.1.5/
  >/var/www/html/index.html

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: 192.168.1.5
Connection: Keep-alive
```

Recommendation

Prevent this information from being displayed to the user.

References

Full Path Disclosure
https://www.owasp.org/index.php/Full_Path_Disclosure

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://192.168.1.5/

Request

```
GET /123ICWG1Dh 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: 192.168.1.5
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

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

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

Integrity Impact	None
Availability Impact	None

User Interaction	None
Scope	Unchanged
Confidentiality	None
Integrity Impact	None
Availability Impact	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://192.168.1.5/

Emails found:

- http://192.168.1.5/wordpress/license.txt
  m@tidakada.com

Request

```
GET /wordpress/license.txt HTTP/1.1
Referer: http://192.168.1.5/wordpress/
Cookie: ec_cart_id=MDCTAOFCQGYAWMTTTLBYBGVKRVGWNX; PHPSESSID=s9c5rtb783s2drgs3465ck7nvr
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: 192.168.1.5
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

WP Support Plus Responsive Ticket System Privilege Escalation

WordPress Plugin WP Support Plus Responsive Ticket System is prone to a privilege escalation vulnerability. Exploiting this issue may allow attackers to bypass the expected capabilities check and perform otherwise restricted actions; other attacks are also possible. WordPress Plugin WP Support Plus Responsive Ticket System version 7.1.4 is vulnerable; prior versions may also be affected.

CWE

CWE-264

CVSS2

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

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

CVSS3

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

Base Score	7.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity Impact	Low
Availability Impact	Low

CVSS4

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

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

Report Confidence	Confirmed

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

Impact

http://192.168.1.5/wordpress/wp-content/plugins/wp-support-plus-responsive-ticket-system/

wp-support-plus-responsive-ticket-system v7.1.3-7.1.3

Recommendation

Update to plugin version 8.0.0 or latest

References

http://security.szurek.pl/wp-support-plus-responsive-ticket-system-713-privilege-escalation.html
http://security.szurek.pl/wp-support-plus-responsive-ticket-system-713-privilege-escalation.html

https://www.exploit-db.com/exploits/41006/
https://www.exploit-db.com/exploits/41006/

https://packetstormsecurity.com/files/140413/WordPress-WP-Support-Plus-Responsive-Ticket-System-7.1.3-Privilege-Escalation.html
https://packetstormsecurity.com/files/140413/WordPress-WP-Support-Plus-Responsive-Ticket-System-7.1.3-Privilege-Escalation.html

Cookies with missing, inconsistent or contradictory properties

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

CWE
CWE-284

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

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

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

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

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

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

Impact

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

http://192.168.1.5/ Verified

List of cookies with missing, inconsistent or contradictory properties:

- http://192.168.1.5/wordpress/

  Cookie was set with:

  ```
  Set-Cookie: PHPSESSID=nt36t21i6j2s3qvn17255ejgni; path=/
  ```

This cookie has the following issues:

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

- http://192.168.1.5/wordpress/

  Cookie was set with:

  ```
  Set-Cookie: ec_cart_id=GBBQYPNKBUSYMSPGDLURKTQEGRKPQF; expires=Wed, 03-Dec-2025 09:13:10 GMT; Max-Age=2592000
  ```

  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://192.168.1.5/wordpress/xmlrpc.php

  Cookie was set with:

  ```
  Set-Cookie: PHPSESSID=24busvcfb909uhjt8582cmnvqc; path=/
  ```

  This cookie has the following issues:

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

- http://192.168.1.5/wordpress/xmlrpc.php

  Cookie was set with:

  ```
  Set-Cookie: ec_cart_id=KMLJISIMSIRGSUWKKGLAZRAGDKWMWD; expires=Wed, 03-Dec-2025 09:18:59 GMT; Max-Age=2592000
  ```

  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://192.168.1.5/wordpress/wp-comments-post.php

  Cookie was set with:

  ```
  Set-Cookie: comment_author_311f7ebdbf2fdff1bfa4c4b8376b4bbf=sOdPqaAH; expires=Fri, 16-Oct-2026 14:41:34 GMT; Max-Age=30000000; path=/wordpress/
  ```

  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://192.168.1.5/wordpress/wp-comments-post.php

  Cookie was set with:

  ```
  Set-Cookie: comment_author_email_311f7ebdbf2fdff1bfa4c4b8376b4bbf=testing%40example.com; expires=Fri, 16-Oct-2026 14:41:34 GMT; Max-Age=30000000; path=/wordpress/
  ```

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://192.168.1.5/wordpress/wp-comments-post.php

  Cookie was set with:

  ```
  Set-Cookie: comment_author_url_311f7ebdbf2fdff1bfa4c4b8376b4bbf=http%3A%2F%2Fwww.example.com; expires=Fri, 16-Oct-2026 14:41:34
  GMT; Max-Age=30000000; path=/wordpress/
  ```

  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://192.168.1.5/wordpress/wp-login.php

  Cookie was set with:

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

  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://192.168.1.5/wordpress/wp-comments-post.php

  Cookie was set with:

  ```
  Set-Cookie: comment_author_311f7ebdbf2fdff1bfa4c4b8376b4bbf=1; expires=Fri, 16-Oct-2026 14:47:09 GMT; Max-Age=30000000;
  path=/wordpress/
  ```

  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://192.168.1.5/wordpress/wp-comments-post.php

  Cookie was set with:

  ```
  Set-Cookie: comment_author_email_311f7ebdbf2fdff1bfa4c4b8376b4bbf=testing%40example.com; expires=Fri, 16-Oct-2026 14:47:09 GMT;
  Max-Age=30000000; path=/wordpress/
  ```

  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://192.168.1.5/wordpress/wp-comments-post.php

  Cookie was set with:

  ```
  Set-Cookie: comment_author_url_311f7ebdbf2fdff1bfa4c4b8376b4bbf=http%3A%2F%2Fwww.example.com; expires=Fri, 16-Oct-2026 14:47:09
  GMT; Max-Age=30000000; path=/wordpress/
  ```

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://192.168.1.5/wordpress/xmlrpc.php

  Cookie was set with:

  ```
  Set-Cookie: PHPSESSID=kdanbgpv3f2aml1tqh21g5vvru; path=/
  ```

  This cookie has the following issues:

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

- http://192.168.1.5/wordpress/xmlrpc.php

  Cookie was set with:

  ```
  Set-Cookie: ec_cart_id=QGVRJYGDZHYXZDLVJFJAKYNRGFPLFZ; expires=Wed, 03-Dec-2025 09:39:04 GMT; Max-Age=2592000
  ```

  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://192.168.1.5/wordpress/xmlrpc.php

  Cookie was set with:

  ```
  Set-Cookie: PHPSESSID=gefo47tpr1q5b188ct9qkrgalk; path=/
  ```

  This cookie has the following issues:

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

- http://192.168.1.5/wordpress/xmlrpc.php

  Cookie was set with:

  ```
  Set-Cookie: ec_cart_id=DAVMQAKFOICTWLBSDXESPLMOZXIDFS; expires=Wed, 03-Dec-2025 09:41:24 GMT; Max-Age=2592000
  ```

  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://192.168.1.5/wordpress/wp-login.php

  Cookie was set with:

  ```
  Set-Cookie: wordpress_311f7ebdbf2fdff1bfa4c4b8376b4bbf=+; expires=Sun, 03-Nov-2024 09:42:02 GMT; Max-Age=0; path=/wordpress/wp-
  admin
  ```

  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://192.168.1.5/wordpress/wp-login.php

  Cookie was set with:

  ```
  Set-Cookie: wordpress_sec_311f7ebdbf2fdff1bfa4c4b8376b4bbf=+; expires=Sun, 03-Nov-2024 09:42:02 GMT; Max-Age=0;
  path=/wordpress/wp-admin
  ```

  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://192.168.1.5/wordpress/wp-login.php

  Cookie was set with:

  ```
  Set-Cookie: wordpress_logged_in_311f7ebdbf2fdff1bfa4c4b8376b4bbf=+; expires=Sun, 03-Nov-2024 09:42:02 GMT; Max-Age=0;
  path=/wordpress/
  ```

  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://192.168.1.5/wordpress/wp-login.php

  Cookie was set with:

  ```
  Set-Cookie: wp-settings-0=+; expires=Sun, 03-Nov-2024 09:42:02 GMT; Max-Age=0; path=/wordpress/
  ```

  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://192.168.1.5/wordpress/wp-login.php

  Cookie was set with:

  ```
  Set-Cookie: wp-settings-time-0=+; expires=Sun, 03-Nov-2024 09:42:02 GMT; Max-Age=0; path=/wordpress/
  ```

  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://192.168.1.5/wordpress/wp-login.php

  Cookie was set with:

  ```
  Set-Cookie: wordpressuser_311f7ebdbf2fdff1bfa4c4b8376b4bbf=+; expires=Sun, 03-Nov-2024 09:42:02 GMT; Max-Age=0; path=/wordpress/
  ```

  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 /wordpress/ HTTP/1.1
Referer: http://192.168.1.5/
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: 192.168.1.5
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

Gwolle Guestbook Multiple Vulnerabilities

WordPress Plugin Gwolle Guestbook is prone to multiple vulnerabilities, including cross-site scripting and cross-site 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 and launch other attacks, or to perform certain administrative actions and gain unauthorized access to the affected application. WordPress Plugin Gwolle Guestbook version 2.1.0 is vulnerable; prior versions may also be affected.

CWE

CWE-352

CVSS2

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

Access Vector	Network
Access Complexity	Medium
Authentication	None
Confidentiality	None
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:N/I:L/A:N

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

CVSS4

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

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

Impact

http://192.168.1.5/wordpress/wp-content/plugins/gwolle-gb/

gwolle-gb v1.5.3-1.5.3

Recommendation

Update to plugin version 2.1.1 or latest

References

https://sumofpwn.nl/advisory/2016/gwolle_guestbook_mass_action_vulnerable_for_cross_site_request_forgery.html
https://sumofpwn.nl/advisory/2016/gwolle_guestbook_mass_action_vulnerable_for_cross_site_request_forgery.html

https://sumofpwn.nl/advisory/2016/cross_site_scripting_vulnerability_in_gwolle_guestbook_wordpress_plugin.html
https://sumofpwn.nl/advisory/2016/cross_site_scripting_vulnerability_in_gwolle_guestbook_wordpress_plugin.html

http://www.openwall.com/lists/oss-security/2017/03/01/4
http://www.openwall.com/lists/oss-security/2017/03/01/4

http://www.openwall.com/lists/oss-security/2017/03/01/3
http://www.openwall.com/lists/oss-security/2017/03/01/3

https://packetstormsecurity.com/files/141416/WordPress-Gwolle-Guestbook-1.7.4-Cross-Site-Request-Forgery.html
https://packetstormsecurity.com/files/141416/WordPress-Gwolle-Guestbook-1.7.4-Cross-Site-Request-Forgery.html

https://packetstormsecurity.com/files/141411/WordPress-Gwolle-Guestbook-1.7.4-Cross-Site-Scripting.html
https://packetstormsecurity.com/files/141411/WordPress-Gwolle-Guestbook-1.7.4-Cross-Site-Scripting.html

https://wordpress.org/plugins/gwolle-gb/changelog/
https://wordpress.org/plugins/gwolle-gb/changelog/

Shopping Cart & eCommerce Store Cross-Site Request Forgery

WordPress Plugin Shopping Cart & eCommerce Store 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 Plugin Shopping Cart & eCommerce Store version 5.1.0 is vulnerable; prior versions may also be affected.

CWE
CWE-352

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

Access Vector	Network
Access Complexity	Medium
Authentication	None
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: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

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://192.168.1.5/wordpress/wp-content/plugins/wp-easycart/

wp-easycart v3.0.4-3.0.4

Recommendation

Update to the latest plugin version

References

https://www.wordfence.com/vulnerability-advisories/#CVE-2021-34645
https://www.wordfence.com/vulnerability-advisories/#CVE-2021-34645

https://plugins.svn.wordpress.org/wp-easycart/trunk/readme.txt
https://plugins.svn.wordpress.org/wp-easycart/trunk/readme.txt

Development configuration files

One or more configuration files (e.g. Vagrantfile, Gemfile, Rakefile, ...) were found. These files may expose sensitive information that could help a malicious user to prepare more advanced attacks. It's recommended to remove or restrict access to this type of 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:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N

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

CVSS4
CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:A/VC:L/VI:N/VA:N/SC:N/SI:N/SA: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	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://192.168.1.5/

Development configuration files:

- http://192.168.1.5/wordpress/wp-content/plugins/site-editor/**package.json**

  ```
  package.json => Grunt configuration file. Grunt is a JavaScript task runner.
  ```

- http://192.168.1.5/wordpress/wp-content/plugins/site-editor/**.gitignore**

  ```
  .gitignore => Git configuration file. Git is a free and open source distributed version control system.
  ```

Request

```
GET /wordpress/wp-content/plugins/site-editor/package.json HTTP/1.1
Cookie: ec_cart_id=GBBQYPNKBUSYMSPGDLURKTQEGRKPQF; PHPSESSID=nt36t21i6j2s3qvn17255ejgni
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: 192.168.1.5
Connection: Keep-alive
```

Recommendation

Remove or restrict access to all configuration files acessible from internet.

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://192.168.1.5/ Verified

Folders with directory listing enabled:

- http://192.168.1.5/wordpress/wp-content/plugins/site-editor/editor/extensions/
- http://192.168.1.5/wordpress/wp-content/plugins/site-editor/editor/extensions/pagebuilder/modules/row/
- http://192.168.1.5/wordpress/wp-content/plugins/site-editor/editor/extensions/pagebuilder/modules/row/js/
- http://192.168.1.5/wordpress/wp-content/plugins/wp-symposium/
- http://192.168.1.5/wordpress/wp-content/plugins/wp-symposium/ajax/
- http://192.168.1.5/wordpress/wp-includes/
- http://192.168.1.5/wordpress/wp-includes/js/
- http://192.168.1.5/wordpress/wp-content/plugins/site-editor/editor/extensions/icon-library/
- http://192.168.1.5/wordpress/wp-content/plugins/site-editor/editor/extensions/icon-library/fonts/
- http://192.168.1.5/wordpress/wp-content/plugins/site-editor/editor/extensions/icon-library/fonts/FontAwesome/
- http://192.168.1.5/wordpress/wp-includes/css/
- http://192.168.1.5/wordpress/wp-includes/css/dist/
- http://192.168.1.5/wordpress/wp-includes/css/dist/block-library/
- http://192.168.1.5/wordpress/wp-content/plugins/wp-support-plus-responsive-ticket-system/
- http://192.168.1.5/wordpress/wp-content/plugins/wp-support-plus-responsive-ticket-system/asset/js/bootstrap/css/
- http://192.168.1.5/wordpress/wp-content/plugins/wp-support-plus-responsive-ticket-system/asset/
- http://192.168.1.5/wordpress/wp-content/plugins/wp-support-plus-responsive-ticket-system/asset/js/
- http://192.168.1.5/wordpress/wp-content/plugins/wp-support-plus-responsive-ticket-system/asset/js/bootstrap/
- http://192.168.1.5/wordpress/wp-admin/css/
- http://192.168.1.5/wordpress/wp-includes/js/jquery/
- http://192.168.1.5/wordpress/wp-includes/js/jquery/ui/

Request

```
GET /wordpress/wp-content/plugins/site-editor/editor/extensions/ HTTP/1.1
Cookie: ec_cart_id=GBBQYPNKBUSYMSPGDLURKTQEGRKPQF; PHPSESSID=nt36t21i6j2s3qvn17255ejgni
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: 192.168.1.5
Connection: Keep-alive
```

Recommendation

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

References

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

Documentation files

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

CWE
CWE-538

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

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

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

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

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

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

Impact

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

http://192.168.1.5/

Documentation files:

- http://192.168.1.5/wordpress/**readme.html**
  File contents (first 100 characters):

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

- http://192.168.1.5/wordpress/**license.txt**
  File contents (first 100 characters):

```
WordPress - Web publishing software

Copyright 2011-2019 by the contributors

This program is fr ...
```

- http://192.168.1.5/wordpress/wp-content/plugins/site-editor/**readme.txt**
  File contents (first 100 characters):

```
=== Site Editor - WordPress Site Builder - Theme Builder and Page Builder ===
Contributors: wpsiteed ...
```

- http://192.168.1.5/wordpress/wp-content/plugins/site-editor/**README.md**
  File contents (first 100 characters):

```
# Site Editor - WordPress Site Builder - Theme Builder and Page Builder


**Contributors:** [wpsitee ...
```

- http://192.168.1.5/wordpress/wp-content/plugins/wp-symposium/**readme.txt**
  File contents (first 100 characters):

```
=== Plugin Name ===
Author: WP Symposium
Contributors: Simon Goodchild
Donate link: http://www.wpsym ...
```

Request

```
GET /wordpress/readme.html HTTP/1.1
Cookie: ec_cart_id=MDCTAOFCQGYAWMTTTLBYBGVKRVGWNX; PHPSESSID=s9c5rtb783s2drgs3465ck7nvr
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: 192.168.1.5
Connection: Keep-alive
```

Recommendation

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

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).

Development configuration files

One or more configuration files (e.g. Vagrantfile, Gemfile, Rakefile, ...) were found. These files may expose sensitive information that could help a malicious user to prepare more advanced attacks. It's recommended to remove or restrict access to this type of 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:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N

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

CVSS4
CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:A/VC:L/VI:N/VA:N/SC:N/SI:N/SA: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	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://192.168.1.5/

Development configuration files:

- http://192.168.1.5/wordpress/wp-content/plugins/site-editor/**package.json**

```
package.json => Grunt configuration file. Grunt is a JavaScript task runner.
```

- http://192.168.1.5/wordpress/wp-content/plugins/site-editor/**.gitignore**

```
.gitignore => Git configuration file. Git is a free and open source distributed version control system.
```

Request

```
GET /wordpress/wp-content/plugins/site-editor/package.json HTTP/1.1
Cookie: ec_cart_id=GBBQYPNKBUSYMSPGDLURKTQEGRKPQF; PHPSESSID=nt36t21i6j2s3qvn17255ejgni
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: 192.168.1.5
Connection: Keep-alive
```

Recommendation

Remove or restrict access to all configuration files acessible from internet.

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://192.168.1.5/ Verified

Folders with directory listing enabled:

- http://192.168.1.5/wordpress/wp-content/plugins/site-editor/editor/extensions/
- http://192.168.1.5/wordpress/wp-content/plugins/site-editor/editor/extensions/pagebuilder/modules/row/
- http://192.168.1.5/wordpress/wp-content/plugins/site-editor/editor/extensions/pagebuilder/modules/row/js/
- http://192.168.1.5/wordpress/wp-content/plugins/wp-symposium/
- http://192.168.1.5/wordpress/wp-content/plugins/wp-symposium/ajax/
- http://192.168.1.5/wordpress/wp-includes/
- http://192.168.1.5/wordpress/wp-includes/js/
- http://192.168.1.5/wordpress/wp-content/plugins/site-editor/editor/extensions/icon-library/
- http://192.168.1.5/wordpress/wp-content/plugins/site-editor/editor/extensions/icon-library/fonts/
- http://192.168.1.5/wordpress/wp-content/plugins/site-editor/editor/extensions/icon-library/fonts/FontAwesome/
- http://192.168.1.5/wordpress/wp-includes/css/
- http://192.168.1.5/wordpress/wp-includes/css/dist/
- http://192.168.1.5/wordpress/wp-includes/css/dist/block-library/
- http://192.168.1.5/wordpress/wp-content/plugins/wp-support-plus-responsive-ticket-system/
- http://192.168.1.5/wordpress/wp-content/plugins/wp-support-plus-responsive-ticket-system/asset/js/bootstrap/css/

- http://192.168.1.5/wordpress/wp-content/plugins/wp-support-plus-responsive-ticket-system/asset/
- http://192.168.1.5/wordpress/wp-content/plugins/wp-support-plus-responsive-ticket-system/asset/js/
- http://192.168.1.5/wordpress/wp-content/plugins/wp-support-plus-responsive-ticket-system/asset/js/bootstrap/
- http://192.168.1.5/wordpress/wp-admin/css/
- http://192.168.1.5/wordpress/wp-includes/js/jquery/
- http://192.168.1.5/wordpress/wp-includes/js/jquery/ui/

Request

```
GET /wordpress/wp-content/plugins/site-editor/editor/extensions/ HTTP/1.1
Cookie: ec_cart_id=GBBQYPNKBUSYMSPGDLURKTQEGRKPQF; PHPSESSID=nt36t21i6j2s3qvn17255ejgni
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: 192.168.1.5
Connection: Keep-alive
```

Recommendation

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

References

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

WordPress username enumeration

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

CWE

CWE-200

CVSS2

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

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

CVSS3

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

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

CVSS4

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

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

Impact

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

http://192.168.1.5/wordpress/

List of WordPress users for {'_nativeUrl': {'password': '', 'username': '', 'search': '', 'protocol': 'http', 'port': '', 'path': '/wordpress/', 'origin': 'http://192.168.1.5', 'href': 'http://192.168.1.5/wordpress/', 'hostname': '192.168.1.5', 'host': '192.168.1.5', 'hash': ''}}:

['admin']

Request

```
POST /wordpress//wp-login.php HTTP/1.1
Content-type: application/x-www-form-urlencoded
Cookie: comment_author_311f7ebdbf2fdff1bfa4c4b8376b4bbf=sOdPqaAH; comment_author_email_311f7ebdbf2fdff1bfa4c4b8376b4bbf=testing%40example.com;
comment_author_url_311f7ebdbf2fdff1bfa4c4b8376b4bbf=http%3A%2F%2Fwww.example.com; ec_cart_id=KRZULVEOJJCQRXPJOVCUNFMMHEFDBE;
PHPSESSID=aqceka9dkvqmo63rrm46ru828b
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: 192.168.1.5
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.

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://192.168.1.5/

Documentation files:

- http://192.168.1.5/wordpress/**readme.html**
  File contents (first 100 characters):

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

- http://192.168.1.5/wordpress/**license.txt**
  File contents (first 100 characters):

```
WordPress - Web publishing software
```

```
Copyright 2011-2019 by the contributors

This program is fr ...
```

- http://192.168.1.5/wordpress/wp-content/plugins/site-editor/**readme.txt**
  File contents (first 100 characters):

```
=== Site Editor - WordPress Site Builder - Theme Builder and Page Builder ===
Contributors: wpsiteed ...
```

- http://192.168.1.5/wordpress/wp-content/plugins/site-editor/**README.md**
  File contents (first 100 characters):

```
# Site Editor - WordPress Site Builder - Theme Builder and Page Builder


**Contributors:** [wpsitee ...
```

- http://192.168.1.5/wordpress/wp-content/plugins/wp-symposium/**readme.txt**
  File contents (first 100 characters):

```
=== Plugin Name ===
Author: WP Symposium
Contributors: Simon Goodchild
Donate link: http://www.wpsym ...
```

Request

```
GET /wordpress/readme.html HTTP/1.1
Cookie: ec_cart_id=MDCTAOFCQGYAWMTTTLBYBGVKRVGWNX; PHPSESSID=s9c5rtb783s2drgs3465ck7nvr
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: 192.168.1.5
Connection: Keep-alive
```

Recommendation

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

Possible sensitive directories

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

CWE
CWE-200

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

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

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

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

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

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

Impact

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

http://192.168.1.5/

Possible sensitive directories:

- http://192.168.1.5/wordpress/wp-content/**uploads**
- http://192.168.1.5/wordpress/wp-content/plugins/site-editor/**includes**
- http://192.168.1.5/wordpress/wp-content/plugins/site-editor/editor/**includes**
- http://192.168.1.5/wordpress/wp-content/plugins/site-editor/editor/extensions/pagebuilder/**includes**

Request

```
GET /wordpress/wp-content/uploads/ HTTP/1.1
Cookie: ec_cart_id=GBBQYPNKBUSYMSPGDLURKTQEGRKPQF; PHPSESSID=nt36t21i6j2s3qvn17255ejgni
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: 192.168.1.5
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/

[Possible] Internal Path Disclosure (*nix)

One or more fully qualified path names were found. From this information the attacker may learn the file system structure from the web server. This information can be used to conduct further attacks.

This alert may be a false positive, manual confirmation is required.

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

Possible sensitive information disclosure.

http://192.168.1.5/

Pages with paths being disclosed:

- http://192.168.1.5/
  >/var/www/html/index.html

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: 192.168.1.5
Connection: Keep-alive
```

Recommendation

Prevent this information from being displayed to the user.

References

Full Path Disclosure
https://www.owasp.org/index.php/Full_Path_Disclosure

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://192.168.1.5/

Request

```
GET /123ICWG1Dh 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: 192.168.1.5
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://192.168.1.5/

Emails found:

- http://192.168.1.5/wordpress/license.txt
  m@tidakada.com

Request

```
GET /wordpress/license.txt HTTP/1.1
Referer: http://192.168.1.5/wordpress/
Cookie: ec_cart_id=MDCTAOFCQGYAWMTTTLBYBGVKRVGWNX; PHPSESSID=s9c5rtb783s2drgs3465ck7nvr
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: 192.168.1.5
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://192.168.1.5/ Verified

Request

```
GET / HTTP/1.1
Referer: http://192.168.1.5/
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: 192.168.1.5
Connection: Keep-alive
```

Recommendation

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

A03 Injection

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

Mail Masta Multiple SQL Injection Vulnerabilities

WordPress Plugin Mail Masta is prone to multiple SQL injection vulnerabilities because it fails to sufficiently sanitize user-supplied data before using it in an SQL query. Exploiting these issues could allow an attacker to compromise the application, access or modify data, or exploit latent vulnerabilities in the underlying database. WordPress Plugin Mail Masta version 1.0 is vulnerable.

CWE
CWE-89

CVSS2
AV:N/AC:L/Au:N/C:P/I:P/A:P/E:POC/RL:U/RC:C

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

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

Base Score	8.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Changed
Confidentiality	Low
Integrity Impact	Low
Availability Impact	Low

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

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

Impact

http://192.168.1.5/wordpress/wp-content/plugins/mail-masta/

mail-masta v1.0-1.0

Recommendation

Edit the source code to ensure that input is properly sanitised or disable the plugin until a fix is available

References

https://github.com/hamkovic/Mail-Masta-Wordpress-Plugin-SQL-Injection-Vulnerability
https://github.com/hamkovic/Mail-Masta-Wordpress-Plugin-SQL-Injection-Vulnerability

https://www.exploit-db.com/exploits/41438/
https://www.exploit-db.com/exploits/41438/

https://packetstormsecurity.com/files/141277/WordPress-Mail-Masta-1.0-SQL-Injection.html
https://packetstormsecurity.com/files/141277/WordPress-Mail-Masta-1.0-SQL-Injection.html

WP Support Plus Responsive Ticket System SQL Injection

WordPress Plugin WP Support Plus Responsive Ticket System is prone to an SQL injection vulnerability because it fails to sufficiently sanitize user-supplied data before using it in an SQL query. Exploiting this issue could allow an attacker to compromise the application, access or modify data, or exploit latent vulnerabilities in the underlying database. WordPress Plugin WP Support Plus Responsive Ticket System version 7.1.4 is vulnerable; prior versions may also be affected.

CWE
CWE-89

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://192.168.1.5/wordpress/wp-content/plugins/wp-support-plus-responsive-ticket-system/

wp-support-plus-responsive-ticket-system v7.1.3-7.1.3

Recommendation

Update to plugin version 7.1.5 or latest

References

http://lenonleite.com.br/en/blog/2016/12/13/wp-support-plus-responsive-ticket-system-wordpress-plugin-sql-injection/
http://lenonleite.com.br/en/blog/2016/12/13/wp-support-plus-responsive-ticket-system-wordpress-plugin-sql-injection/

https://www.exploit-db.com/exploits/40939/
https://www.exploit-db.com/exploits/40939/

https://packetstormsecurity.com/files/140203/WordPress-Support-Plus-Responsive-Ticket-System-7.1.3-SQL-Injection.html
https://packetstormsecurity.com/files/140203/WordPress-Support-Plus-Responsive-Ticket-System-7.1.3-SQL-Injection.html

https://wordpress.org/plugins/wp-support-plus-responsive-ticket-system/changelog/
https://wordpress.org/plugins/wp-support-plus-responsive-ticket-system/changelog/

WP Symposium SQL Injection

WordPress Plugin WP Symposium is prone to an SQL injection vulnerability because it fails to sufficiently sanitize user-supplied data before using it in an SQL query. Exploiting this issue could allow an attacker to compromise the application, access or modify data, or exploit latent vulnerabilities in the underlying database. WordPress Plugin WP Symposium version 15.5.1 is vulnerable; prior versions may also be affected.

CWE

CWE-89

CVSS2

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

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

CVSS3

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

Base Score	10
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Changed
Confidentiality	High
Integrity Impact	High
Availability Impact	None

CVSS4

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

Report Confidence	Confirmed

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

Impact

http://192.168.1.5/wordpress/wp-content/plugins/wp-symposium/

wp-symposium v15.1-15.1

http://192.168.1.5/wordpress/wp-content/plugins/wp-symposium/

wp-symposium v15.1-15.1

Recommendation

Update to plugin version 15.8 or latest

References

https://security.dxw.com/advisories/blind-sql-injection-in-wp-symposium-allows-unauthenticated-attackers-to-access-sensitive-data/
https://security.dxw.com/advisories/blind-sql-injection-in-wp-symposium-allows-unauthenticated-attackers-to-access-sensitive-data/

https://www.exploit-db.com/exploits/37822/
https://www.exploit-db.com/exploits/37822/

https://packetstormsecurity.com/files/133047/WordPress-WP-Symposium-15.1-SQL-Injection.html
https://packetstormsecurity.com/files/133047/WordPress-WP-Symposium-15.1-SQL-Injection.html

https://www.exploit-db.com/exploits/37824/
https://www.exploit-db.com/exploits/37824/

Gwolle Guestbook Cross-Site Scripting

WordPress Plugin Gwolle Guestbook is prone to a cross-site scripting vulnerability because it fails to properly sanitize user-supplied input. 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. This can allow the attacker to steal cookie-based authentication credentials and launch other attacks. WordPress Plugin Gwolle Guestbook version 2.5.3 is vulnerable; prior versions may also be affected.

CWE
CWE-79

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

Access Vector	Network
Access Complexity	Medium
Authentication	Single
Confidentiality	None
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: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/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	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://192.168.1.5/wordpress/wp-content/plugins/gwolle-gb/

gwolle-gb v1.5.3-1.5.3

Recommendation

Update to plugin version 2.5.4 or latest

References

http://www.defensecode.com/advisories/DC-2018-05-008_WordPress_Gwolle_Guestbook_Plugin_Advisory.pdf
http://www.defensecode.com/advisories/DC-2018-05-008_WordPress_Gwolle_Guestbook_Plugin_Advisory.pdf

https://packetstormsecurity.com/files/148715/WordPress-Gwolle-Guestbook-2.5.3-Cross-Site-Scripting.html
https://packetstormsecurity.com/files/148715/WordPress-Gwolle-Guestbook-2.5.3-Cross-Site-Scripting.html

https://plugins.svn.wordpress.org/gwolle-gb/trunk/readme.txt
https://plugins.svn.wordpress.org/gwolle-gb/trunk/readme.txt

ReFlex Gallery Cross-Site Scripting

WordPress Plugin ReFlex Gallery is prone to a cross-site scripting vulnerability because it fails to properly sanitize user-supplied input. 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. This can allow the attacker to steal cookie-based authentication credentials and launch other attacks. WordPress Plugin ReFlex Gallery version 3.1.4 is vulnerable; prior versions may also be affected.

CWE
CWE-79

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

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

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

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

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:P/VC:N/VI:L/VA:N/SC: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	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://192.168.1.5/wordpress/wp-content/plugins/reflex-gallery/

reflex-gallery v3.1.3-3.1.3

Recommendation

Update to plugin version 3.1.5 or latest

References

https://blog.anantshri.info/forgotten_disclosure_dom_xss_prettyphoto
https://blog.anantshri.info/forgotten_disclosure_dom_xss_prettyphoto

https://github.com/wpscanteam/wpscan/issues/818
https://github.com/wpscanteam/wpscan/issues/818

https://github.com/scaron/prettyphoto/issues/149
https://github.com/scaron/prettyphoto/issues/149

http://www.perucrack.net/2014/07/haciendo-un-xss-en-plugin-prettyphoto.html
http://www.perucrack.net/2014/07/haciendo-un-xss-en-plugin-prettyphoto.html

Slideshow Gallery LITE Cross-Site Scripting

WordPress Plugin Slideshow Gallery LITE is prone to a cross-site scripting vulnerability because it fails to properly sanitize user-supplied input. 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. This can allow the attacker to steal cookie-based authentication credentials and launch other attacks. WordPress Plugin Slideshow Gallery LITE version 1.5.3.4 is vulnerable; prior versions may also be affected.

CWE
CWE-79

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

Access Vector	Network
Access Complexity	Medium
Authentication	Single
Confidentiality	None
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: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/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	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://192.168.1.5/wordpress/wp-content/plugins/slideshow-gallery/
slideshow-gallery v1.4.6-1.4.6

http://192.168.1.5/wordpress/wp-content/plugins/slideshow-gallery/
slideshow-gallery v1.4.6-1.4.6

http://192.168.1.5/wordpress/wp-content/plugins/slideshow-gallery/
slideshow-gallery v1.4.6-1.4.6

Recommendation

Update to plugin version 1.6.1 or latest

References

http://security.szurek.pl/tribulant-slideshow-gallery-1534-reflected-xss.html
http://security.szurek.pl/tribulant-slideshow-gallery-1534-reflected-xss.html

https://wordpress.org/plugins/slideshow-gallery/changelog/
https://wordpress.org/plugins/slideshow-gallery/changelog/

Slideshow Gallery LITE Multiple Cross-Site Scripting Vulnerabilities

WordPress Plugin Slideshow Gallery LITE is prone to multiple cross-site scripting vulnerabilities because it fails to properly sanitize user-supplied input. 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. This can allow the attacker to steal cookie-based authentication credentials and launch other attacks. WordPress Plugin Slideshow Gallery LITE version 1.6.5 is vulnerable; prior versions may also be affected.

CWE
CWE-79

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

Access Vector	Network
Access Complexity	Medium

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

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

Base Score	4.8
Attack Vector	Network

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

Attack Complexity	Low
Privileges Required	Low
User Interaction	Required
Scope	Changed
Confidentiality	None
Integrity Impact	Low
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	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://192.168.1.5/wordpress/wp-content/plugins/slideshow-gallery/

slideshow-gallery v1.4.6-1.4.6

Recommendation

Update to plugin version 1.6.6.1 or latest

References

http://www.defensecode.com/advisories/DC-2017-01-014_WordPress_Tribulant_Slideshow_Gallery_Plugin_Advisory.pdf
http://www.defensecode.com/advisories/DC-2017-01-014_WordPress_Tribulant_Slideshow_Gallery_Plugin_Advisory.pdf

https://packetstormsecurity.com/files/142079/WordPress-Tribulant-Slideshow-Gallery-1.6.5-Cross-Site-Scripting.html
https://packetstormsecurity.com/files/142079/WordPress-Tribulant-Slideshow-Gallery-1.6.5-Cross-Site-Scripting.html

https://wordpress.org/plugins/slideshow-gallery/#changelog
https://wordpress.org/plugins/slideshow-gallery/#changelog

WP Support Plus Responsive Ticket System Cross-Site Scripting

WordPress Plugin WP Support Plus Responsive Ticket System is prone to a cross-site scripting vulnerability because it fails to properly sanitize user-supplied input. 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. This can allow the attacker to steal cookie-based authentication credentials and launch other attacks. WordPress Plugin WP Support Plus Responsive Ticket System version 9.1.1 is vulnerable; prior versions may also be affected.

CWE

CWE-79

CVSS2

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

Access Vector	Network
Access Complexity	Medium
Authentication	None
Confidentiality	None
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:N/I:L/A:N

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

CVSS4

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

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

Impact

http://192.168.1.5/wordpress/wp-content/plugins/wp-support-plus-responsive-ticket-system/

wp-support-plus-responsive-ticket-system v7.1.3-7.1.3

Recommendation

Update to plugin version 9.1.2 or latest

References

https://cert.kalasag.com.ph/news/research/cve-2019-7299-stored-xss-in-wp-support-plus-responsive-ticket-system/
https://cert.kalasag.com.ph/news/research/cve-2019-7299-stored-xss-in-wp-support-plus-responsive-ticket-system/

https://plugins.svn.wordpress.org/wp-support-plus-responsive-ticket-system/trunk/readme.txt
https://plugins.svn.wordpress.org/wp-support-plus-responsive-ticket-system/trunk/readme.txt

WP Symposium Cross-Site Scripting

WordPress Plugin WP Symposium is prone to a cross-site scripting vulnerability because it fails to properly sanitize user-supplied input. 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. This can allow the attacker to steal cookie-based authentication credentials and launch other attacks. WordPress Plugin WP Symposium version 15.8.1 is vulnerable; prior versions may also be affected.

CWE
CWE-79

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

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

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

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

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:P/VC:N/VI:L/VA:N/SC: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	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://192.168.1.5/wordpress/wp-content/plugins/wp-symposium/

wp-symposium v15.1-15.1

Recommendation

Edit the source code to ensure that input is properly sanitised or disable the plugin until a fix is available

References

http://cxsecurity.com/issue/WLB-2015090024
http://cxsecurity.com/issue/WLB-2015090024

Slideshow Gallery LITE Arbitrary File Upload

WordPress Plugin Slideshow Gallery LITE is prone to a vulnerability that lets attackers upload arbitrary files. The issue occurs because the application fails to adequately sanitize user-supplied input. An attacker can exploit this vulnerability to upload arbitrary code and run it in the context of the webserver process. This may facilitate unauthorized access or privilege escalation; other attacks are also possible. WordPress Plugin Slideshow Gallery LITE version 1.4.6 is vulnerable; prior versions may also be affected.

CWE
CWE-20

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

Access Vector	Network
Access Complexity	Low
Authentication	Single
Confidentiality	Partial
Integrity Impact	Partial
Availability Impact	Partial
Exploitability	Functional exploit exists
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/SA

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://192.168.1.5/wordpress/wp-content/plugins/slideshow-gallery/

slideshow-gallery v1.4.6-1.4.6

Recommendation

Update to plugin version 1.4.7 or latest

References

http://whitexploit.blogspot.mx/2014/08/wordpress-slideshow-gallery-146-shell.html
http://whitexploit.blogspot.mx/2014/08/wordpress-slideshow-gallery-146-shell.html

http://www.exploit-db.com/exploits/34514/
http://www.exploit-db.com/exploits/34514/

http://www.exploit-db.com/exploits/34681/
http://www.exploit-db.com/exploits/34681/

http://packetstormsecurity.com/files/128069/WordPress-Slideshow-Gallery-1.4.6-Shell-Upload.html
http://packetstormsecurity.com/files/128069/WordPress-Slideshow-Gallery-1.4.6-Shell-Upload.html

http://packetstormsecurity.com/files/131526/WordPress-SlideShow-Gallery-Authenticated-File-Upload.html
http://packetstormsecurity.com/files/131526/WordPress-SlideShow-Gallery-Authenticated-File-Upload.html

http://secunia.com/advisories/60074/
http://secunia.com/advisories/60074/

Gwolle Guestbook Multiple Vulnerabilities

WordPress Plugin Gwolle Guestbook is prone to multiple vulnerabilities, including cross-site scripting and cross-site 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 and launch other attacks, or to perform certain administrative actions and gain unauthorized access to the affected application. WordPress Plugin Gwolle Guestbook version 2.1.0 is vulnerable; prior versions may also be affected.

CWE
CWE-352

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

Access Vector	Network
Access Complexity	Medium

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

Base Score	4.7
Attack Vector	Network

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

Base Score	5.1
Attack Vector	Network

Authentication	None
Confidentiality	None
Integrity Impact	Partial
Availability Impact	None
Exploitability	Proof of concept code
Remediation Level	Official Fix
Report Confidence	Confirmed

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

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

Impact

http://192.168.1.5/wordpress/wp-content/plugins/gwolle-gb/

gwolle-gb v1.5.3-1.5.3

Recommendation

Update to plugin version 2.1.1 or latest

References

https://sumofpwn.nl/advisory/2016/gwolle_guestbook_mass_action_vulnerable_for_cross_site_request_forgery.html
https://sumofpwn.nl/advisory/2016/gwolle_guestbook_mass_action_vulnerable_for_cross_site_request_forgery.html

https://sumofpwn.nl/advisory/2016/cross_site_scripting_vulnerability_in_gwolle_guestbook_wordpress_plugin.html
https://sumofpwn.nl/advisory/2016/cross_site_scripting_vulnerability_in_gwolle_guestbook_wordpress_plugin.html

http://www.openwall.com/lists/oss-security/2017/03/01/4
http://www.openwall.com/lists/oss-security/2017/03/01/4

http://www.openwall.com/lists/oss-security/2017/03/01/3
http://www.openwall.com/lists/oss-security/2017/03/01/3

https://packetstormsecurity.com/files/141416/WordPress-Gwolle-Guestbook-1.7.4-Cross-Site-Request-Forgery.html
https://packetstormsecurity.com/files/141416/WordPress-Gwolle-Guestbook-1.7.4-Cross-Site-Request-Forgery.html

https://packetstormsecurity.com/files/141411/WordPress-Gwolle-Guestbook-1.7.4-Cross-Site-Scripting.html
https://packetstormsecurity.com/files/141411/WordPress-Gwolle-Guestbook-1.7.4-Cross-Site-Scripting.html

https://wordpress.org/plugins/gwolle-gb/changelog/
https://wordpress.org/plugins/gwolle-gb/changelog/

Slideshow Gallery LITE Multiple Vulnerabilities

WordPress Plugin Slideshow Gallery LITE is prone to multiple vulnerabilities, including cross-site scripting and SQL injection vulnerabilities. Exploiting these issues could allow an attacker to execute arbitrary script code in the browser of an unsuspecting user in the context of the affected site, allowing the attacker to steal cookie-based authentication credentials, or to compromise the application, access or modify data, or exploit latent vulnerabilities in the underlying database. WordPress Plugin Slideshow Gallery LITE version 1.6.8 is vulnerable; prior versions may also be affected.

CWE

CWE-89

CVSS2

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

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

CVSS3

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

Base Score	7.1
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	Required
Scope	Changed
Confidentiality	Low
Integrity 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:N/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	Low
Integrity Impact to the Vulnerable System	Low

Report Confidence	Confirmed

Availability Impact	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://192.168.1.5/wordpress/wp-content/plugins/slideshow-gallery/

slideshow-gallery v1.4.6-1.4.6

http://192.168.1.5/wordpress/wp-content/plugins/slideshow-gallery/

slideshow-gallery v1.4.6-1.4.6

http://192.168.1.5/wordpress/wp-content/plugins/slideshow-gallery/

slideshow-gallery v1.4.6-1.4.6

Recommendation

Update to plugin version 1.6.9 or latest

References

https://plugins.svn.wordpress.org/slideshow-gallery/trunk/readme.txt
https://plugins.svn.wordpress.org/slideshow-gallery/trunk/readme.txt

Underscore.js Improper Control of Generation of Code ('Code Injection') Vulnerability

The package underscore from 1.13.0-0 and before 1.13.0-2, from 1.3.2 and before 1.12.1 are vulnerable to Arbitrary Code Injection via the template function, particularly when a variable property is passed as an argument as it is not sanitized.

CWE

CWE-94

CVSS3

CVSS:3.1/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://192.168.1.5/

underscore.js v1.8.3-1.8.3

References

CVE-2021-23358
https://nvd.nist.gov/vuln/detail/CVE-2021-23358

Gwolle Guestbook Remote File Inclusion

WordPress Plugin Gwolle Guestbook is prone to a remote file inclusion vulnerability because it fails to properly verify user-supplied input. An attacker can exploit this issue to include arbitrary remote files containing malicious PHP code and execute it in the context of the webserver process. This may allow the attacker to compromise the application and to gain access to the underlying system. WordPress Plugin Gwolle Guestbook version 1.5.3 is vulnerable; prior versions may also be affected.

CWE
CWE-98

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

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

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

Base Score	9
Attack Vector	Network
Attack Complexity	High
Privileges Required	None
User Interaction	None
Scope	Changed
Confidentiality	High
Integrity Impact	High
Availability Impact	High

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

Base Score	9.2
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	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://192.168.1.5/wordpress/wp-content/plugins/gwolle-gb/

gwolle-gb v1.5.3-1.5.3

Recommendation

Update to plugin version 1.5.4 or latest

References

https://www.htbridge.com/advisory/HTB23275
https://www.htbridge.com/advisory/HTB23275

https://www.exploit-db.com/exploits/38861/
https://www.exploit-db.com/exploits/38861/

https://packetstormsecurity.com/files/134599/WordPress-Gwolle-Guestbook-1.5.3-Remote-File-Inclusion.html
https://packetstormsecurity.com/files/134599/WordPress-Gwolle-Guestbook-1.5.3-Remote-File-Inclusion.html

https://wordpress.org/plugins/gwolle-gb/changelog/
https://wordpress.org/plugins/gwolle-gb/changelog/

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.

ReFlex Gallery Arbitrary File Upload

WordPress Plugin ReFlex Gallery is prone to a vulnerability that lets attackers upload arbitrary files because the application fails to properly sanitize user-supplied input. An attacker can exploit this vulnerability to upload arbitrary code and run it in the context of the webserver process. This may facilitate unauthorized access or privilege escalation; other attacks are also possible. WordPress Plugin ReFlex Gallery version 3.1.3 is vulnerable; prior versions may also be affected.

CWE
CWE-434

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

Access Vector	Network
Access Complexity	Low
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:C/C:L/I:L/A:L

Base Score	8.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Changed
Confidentiality	Low
Integrity Impact	Low
Availability Impact	Low

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

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

Impact

http://192.168.1.5/wordpress/wp-content/plugins/reflex-gallery/

reflex-gallery v3.1.3-3.1.3

Recommendation

Update to plugin version 3.1.4 or latest

References

http://www.exploit-db.com/exploits/36374/
http://www.exploit-db.com/exploits/36374/

http://packetstormsecurity.com/files/130845/WordPress-Reflex-Gallery-3.1.3-Shell-Upload.html
http://packetstormsecurity.com/files/130845/WordPress-Reflex-Gallery-3.1.3-Shell-Upload.html

https://github.com/googleinurl/Wordpress-Plugin-Reflex-Gallery-Arbitrary-File-Upload
https://github.com/googleinurl/Wordpress-Plugin-Reflex-Gallery-Arbitrary-File-Upload

http://packetstormsecurity.com/files/131515/WordPress-Reflex-Gallery-Upload.html
http://packetstormsecurity.com/files/131515/WordPress-Reflex-Gallery-Upload.html

https://www.exploit-db.com/exploits/36809/
https://www.exploit-db.com/exploits/36809/

Shopping Cart & eCommerce Store Arbitrary File Upload

WordPress Plugin Shopping Cart & eCommerce Store is prone to a vulnerability that lets attackers upload arbitrary files because the application fails to properly sanitize user-supplied input. An attacker can exploit this vulnerability to upload arbitrary code and run it in the context of the webserver process. This may facilitate unauthorized access or privilege escalation; other attacks are also possible. WordPress Plugin Shopping Cart & eCommerce Store version 3.0.8 is vulnerable; prior versions may also be affected.

CWE
CWE-434

CVSS2
AV:N/AC:L/Au:S/C:C/I:C/A:N/E:F/RL:OF/RC:C

Access Vector	Network
Access Complexity	Low
Authentication	Single
Confidentiality	Complete
Integrity Impact	Complete
Availability Impact	None
Exploitability	Functional exploit exists
Remediation Level	Official Fix
Report Confidence	Confirmed

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

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

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

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

Impact

http://192.168.1.5/wordpress/wp-content/plugins/wp-easycart/

wp-easycart v3.0.4-3.0.4

Recommendation

Update to plugin version 3.0.9 or latest

References

http://security.szurek.pl/wordpress-shopping-cart-304-unrestricted-file-upload.html
http://security.szurek.pl/wordpress-shopping-cart-304-unrestricted-file-upload.html

http://www.exploit-db.com/exploits/35730/
http://www.exploit-db.com/exploits/35730/

http://packetstormsecurity.com/files/129875/WordPress-Shopping-Cart-3.0.4-Unrestricted-File-Upload.html
http://packetstormsecurity.com/files/129875/WordPress-Shopping-Cart-3.0.4-Unrestricted-File-Upload.html

http://www.exploit-db.com/exploits/36043/
http://www.exploit-db.com/exploits/36043/

http://packetstormsecurity.com/files/130328/WordPress-WP-EasyCart-Unrestricted-File-Upload.html
http://packetstormsecurity.com/files/130328/WordPress-WP-EasyCart-Unrestricted-File-Upload.html

Slideshow Gallery LITE Multiple Vulnerabilities

WordPress Plugin Slideshow Gallery LITE is prone to multiple vulnerabilities, including cross-site scripting and arbitrary file upload 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 launch other attacks, or to upload arbitrary code and run it in the context of the webserver process, which may facilitate unauthorized access or privilege escalation. WordPress Plugin Slideshow Gallery LITE version 1.5.3 is vulnerable; prior versions may also be affected.

CWE
CWE-434

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

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

Base Score	9.1
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:N/VC:H/VI:H/VA:N/SC:N/S

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

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

Confidentiality	High
Integrity Impact	High
Availability Impact	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://192.168.1.5/wordpress/wp-content/plugins/slideshow-gallery/

slideshow-gallery v1.4.6-1.4.6

Recommendation

Update to plugin version 1.5.3.4 or latest

References

http://cinu.pl/research/wp-plugins/mail_5954cbf04cd033877e5415a0c6fba532.html
http://cinu.pl/research/wp-plugins/mail_5954cbf04cd033877e5415a0c6fba532.html

https://wordpress.org/plugins/slideshow-gallery/changelog/
https://wordpress.org/plugins/slideshow-gallery/changelog/

Content Security Policy (CSP) Not Implemented

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

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

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

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

CWE
CWE-1021

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

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

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

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

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

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

Impact

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

http://192.168.1.5/

Paths without CSP header:

- http://192.168.1.5/
- http://192.168.1.5/manual
- http://192.168.1.5/wordpress/
- http://192.168.1.5/wordpress/readme.html
- http://192.168.1.5/wordpress/index.php/2019/09/09/hello-world/
- http://192.168.1.5/wordpress/wp-admin/images/
- http://192.168.1.5/wordpress/wp-admin/install.php
- http://192.168.1.5/wordpress/wp-includes/
- http://192.168.1.5/wordpress/wp-admin/upgrade.php
- http://192.168.1.5/wordpress/wp-login.php
- http://192.168.1.5/wordpress/wp-includes/ID3/
- http://192.168.1.5/wordpress/index.php/author/admin/
- http://192.168.1.5/wordpress/wp-includes/ID3/getid3.lib.php
- http://192.168.1.5/wordpress/index.php/category/uncategorized/

Request

```
GET / HTTP/1.1
Referer: http://192.168.1.5/
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: 192.168.1.5
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	CVSS3	CVSS4
AV:N/AC:L/Au:N/C:N/I:N/A:N	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:N/A:N	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

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://192.168.1.5/

Locations without Permissions-Policy header:

- http://192.168.1.5/
- http://192.168.1.5/icons/
- http://192.168.1.5/manual
- http://192.168.1.5/wordpress/
- http://192.168.1.5/wordpress/readme.html
- http://192.168.1.5/wordpress/wp-content/plugins/wp-symposium/ajax/symposium_ajax_functions.php
- http://192.168.1.5/wordpress/wp-content/plugins/wp-symposium/ajax/symposium_mail_functions.php
- http://192.168.1.5/wordpress/index.php/2019/09/09/hello-world/
- http://192.168.1.5/wordpress/wp-comments-post.php
- http://192.168.1.5/wordpress/wp-login.php
- http://192.168.1.5/wordpress/wp-admin/images/
- http://192.168.1.5/wordpress/wp-admin/install.php
- http://192.168.1.5/wordpress/wp-includes/
- http://192.168.1.5/wordpress/wp-admin/upgrade.php
- http://192.168.1.5/wordpress/wp-includes/ID3/
- http://192.168.1.5/wordpress/index.php/author/admin/
- http://192.168.1.5/wordpress/wp-includes/ID3/getid3.lib.php
- http://192.168.1.5/wordpress/index.php/category/uncategorized/

Request

```
GET / HTTP/1.1
Referer: http://192.168.1.5/
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: 192.168.1.5
Connection: Keep-alive
```

References

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

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

A05 Security Misconfiguration

Security misconfiguration is commonly a result of insecure default configurations, incomplete or ad hoc configurations, open cloud storage, misconfigured HTTP headers, and verbose error messages containing sensitive information. Not only must all operating systems, frameworks, libraries,

and applications be securly configured, but they must be patched and upgraded in a timely fashion.

Directory listings

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

CWE
CWE-538

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

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

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

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

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

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

Impact

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

http://192.168.1.5/ Verified

Folders with directory listing enabled:

- http://192.168.1.5/wordpress/wp-content/plugins/site-editor/editor/extensions/
- http://192.168.1.5/wordpress/wp-content/plugins/site-editor/editor/extensions/pagebuilder/modules/row/
- http://192.168.1.5/wordpress/wp-content/plugins/site-editor/editor/extensions/pagebuilder/modules/row/js/
- http://192.168.1.5/wordpress/wp-content/plugins/wp-symposium/
- http://192.168.1.5/wordpress/wp-content/plugins/wp-symposium/ajax/
- http://192.168.1.5/wordpress/wp-includes/
- http://192.168.1.5/wordpress/wp-includes/js/
- http://192.168.1.5/wordpress/wp-content/plugins/site-editor/editor/extensions/icon-library/
- http://192.168.1.5/wordpress/wp-content/plugins/site-editor/editor/extensions/icon-library/fonts/
- http://192.168.1.5/wordpress/wp-content/plugins/site-editor/editor/extensions/icon-library/fonts/FontAwesome/
- http://192.168.1.5/wordpress/wp-includes/css/
- http://192.168.1.5/wordpress/wp-includes/css/dist/
- http://192.168.1.5/wordpress/wp-includes/css/dist/block-library/
- http://192.168.1.5/wordpress/wp-content/plugins/wp-support-plus-responsive-ticket-system/
- http://192.168.1.5/wordpress/wp-content/plugins/wp-support-plus-responsive-ticket-system/asset/js/bootstrap/css/
- http://192.168.1.5/wordpress/wp-content/plugins/wp-support-plus-responsive-ticket-system/asset/
- http://192.168.1.5/wordpress/wp-content/plugins/wp-support-plus-responsive-ticket-system/asset/js/
- http://192.168.1.5/wordpress/wp-content/plugins/wp-support-plus-responsive-ticket-system/asset/js/bootstrap/
- http://192.168.1.5/wordpress/wp-admin/css/
- http://192.168.1.5/wordpress/wp-includes/js/jquery/
- http://192.168.1.5/wordpress/wp-includes/js/jquery/ui/

Request

```
GET /wordpress/wp-content/plugins/site-editor/editor/extensions/ HTTP/1.1
Cookie: ec_cart_id=GBBQYPNKBUSYMSPGDLURKTQEGRKPQF; PHPSESSID=nt36t21i6j2s3qvn17255ejgni
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: 192.168.1.5
```

```
Connection: Keep-alive
```

Recommendation

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

References

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

Cookies Not Marked as HttpOnly

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

CWE
CWE-1004

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

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

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

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

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

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

Impact

Cookies can be accessed by client-side scripts.

http://192.168.1.5/ Verified

Cookies without HttpOnly flag set:

- http://192.168.1.5/wordpress/

```
Set-Cookie: PHPSESSID=nt36t21i6j2s3qvn17255ejgni; path=/
```

- http://192.168.1.5/wordpress/

```
Set-Cookie: ec_cart_id=GBBQYPNKBUSYMSPGDLURKTQEGRKPQF; expires=Wed, 03-Dec-2025 09:13:10 GMT; Max-Age=2592000
```

- http://192.168.1.5/wordpress/xmlrpc.php

```
Set-Cookie: PHPSESSID=24busvcfb909uhjt8582cmnvqc; path=/
```

- http://192.168.1.5/wordpress/xmlrpc.php

```
Set-Cookie: ec_cart_id=KMLJISIMSIRGSUWKKGLAZRAGDKWMWD; expires=Wed, 03-Dec-2025 09:18:59 GMT; Max-Age=2592000
```

- http://192.168.1.5/wordpress/wp-comments-post.php

  ```
  Set-Cookie: comment_author_311f7ebdbf2fdff1bfa4c4b8376b4bbf=sOdPqaAH; expires=Fri, 16-Oct-2026 14:41:34 GMT; Max-Age=30000000; path=/wordpress/
  ```

- http://192.168.1.5/wordpress/wp-comments-post.php

  ```
  Set-Cookie: comment_author_email_311f7ebdbf2fdff1bfa4c4b8376b4bbf=testing%40example.com; expires=Fri, 16-Oct-2026 14:41:34 GMT; Max-Age=30000000; path=/wordpress/
  ```

- http://192.168.1.5/wordpress/wp-comments-post.php

  ```
  Set-Cookie: comment_author_url_311f7ebdbf2fdff1bfa4c4b8376b4bbf=http%3A%2F%2Fwww.example.com; expires=Fri, 16-Oct-2026 14:41:34 GMT; Max-Age=30000000; path=/wordpress/
  ```

- http://192.168.1.5/wordpress/wp-login.php

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

- http://192.168.1.5/wordpress/wp-comments-post.php

  ```
  Set-Cookie: comment_author_311f7ebdbf2fdff1bfa4c4b8376b4bbf=1; expires=Fri, 16-Oct-2026 14:47:09 GMT; Max-Age=30000000; path=/wordpress/
  ```

- http://192.168.1.5/wordpress/wp-comments-post.php

  ```
  Set-Cookie: comment_author_email_311f7ebdbf2fdff1bfa4c4b8376b4bbf=testing%40example.com; expires=Fri, 16-Oct-2026 14:47:09 GMT; Max-Age=30000000; path=/wordpress/
  ```

- http://192.168.1.5/wordpress/wp-comments-post.php

  ```
  Set-Cookie: comment_author_url_311f7ebdbf2fdff1bfa4c4b8376b4bbf=http%3A%2F%2Fwww.example.com; expires=Fri, 16-Oct-2026 14:47:09 GMT; Max-Age=30000000; path=/wordpress/
  ```

- http://192.168.1.5/wordpress/xmlrpc.php

  ```
  Set-Cookie: PHPSESSID=kdanbgpv3f2aml1tqh21g5vvru; path=/
  ```

- http://192.168.1.5/wordpress/xmlrpc.php

  ```
  Set-Cookie: ec_cart_id=QGVRJYGDZHYXZDLVJFJAKYNRGFPLFZ; expires=Wed, 03-Dec-2025 09:39:04 GMT; Max-Age=2592000
  ```

- http://192.168.1.5/wordpress/xmlrpc.php

  ```
  Set-Cookie: PHPSESSID=gefo47tpr1q5b188ct9qkrgalk; path=/
  ```

- http://192.168.1.5/wordpress/xmlrpc.php

  ```
  Set-Cookie: ec_cart_id=DAVMQAKFOICTWLBSDXESPLMOZXIDFS; expires=Wed, 03-Dec-2025 09:41:24 GMT; Max-Age=2592000
  ```

- http://192.168.1.5/wordpress/wp-login.php

```
Set-Cookie: wordpress_311f7ebdbf2fdff1bfa4c4b8376b4bbf=+; expires=Sun, 03-Nov-2024 09:42:02 GMT; Max-Age=0; path=/wordpress/wp-admin
Set-Cookie: wordpress_311f7ebdbf2fdff1bfa4c4b8376b4bbf=+; expires=Sun, 03-Nov-2024 09:42:02 GMT; Max-Age=0; path=/wordpress/wp-content/plugins
Set-Cookie: wordpress_311f7ebdbf2fdff1bfa4c4b8376b4bbf=+; expires=Sun, 03-Nov-2024 09:42:02 GMT; Max-Age=0; path=/wordpress/
Set-Cookie: wordpress_311f7ebdbf2fdff1bfa4c4b8376b4bbf=+; expires=Sun, 03-Nov-2024 09:42:02 GMT; Max-Age=0; path=/wordpress/
```

- http://192.168.1.5/wordpress/wp-login.php

```
Set-Cookie: wordpress_sec_311f7ebdbf2fdff1bfa4c4b8376b4bbf=+; expires=Sun, 03-Nov-2024 09:42:02 GMT; Max-Age=0; path=/wordpress/wp-admin
Set-Cookie: wordpress_sec_311f7ebdbf2fdff1bfa4c4b8376b4bbf=+; expires=Sun, 03-Nov-2024 09:42:02 GMT; Max-Age=0; path=/wordpress/wp-content/plugins
Set-Cookie: wordpress_sec_311f7ebdbf2fdff1bfa4c4b8376b4bbf=+; expires=Sun, 03-Nov-2024 09:42:02 GMT; Max-Age=0; path=/wordpress/
Set-Cookie: wordpress_sec_311f7ebdbf2fdff1bfa4c4b8376b4bbf=+; expires=Sun, 03-Nov-2024 09:42:02 GMT; Max-Age=0; path=/wordpress/
```

- http://192.168.1.5/wordpress/wp-login.php

```
Set-Cookie: wordpress_logged_in_311f7ebdbf2fdff1bfa4c4b8376b4bbf=+; expires=Sun, 03-Nov-2024 09:42:02 GMT; Max-Age=0; path=/wordpress/
Set-Cookie: wordpress_logged_in_311f7ebdbf2fdff1bfa4c4b8376b4bbf=+; expires=Sun, 03-Nov-2024 09:42:02 GMT; Max-Age=0; path=/wordpress/
```

- http://192.168.1.5/wordpress/wp-login.php

```
Set-Cookie: wp-settings-0=+; expires=Sun, 03-Nov-2024 09:42:02 GMT; Max-Age=0; path=/wordpress/
```

- http://192.168.1.5/wordpress/wp-login.php

```
Set-Cookie: wp-settings-time-0=+; expires=Sun, 03-Nov-2024 09:42:02 GMT; Max-Age=0; path=/wordpress/
```

- http://192.168.1.5/wordpress/wp-login.php

```
Set-Cookie: wordpressuser_311f7ebdbf2fdff1bfa4c4b8376b4bbf=+; expires=Sun, 03-Nov-2024 09:42:02 GMT; Max-Age=0; path=/wordpress/
Set-Cookie: wordpressuser_311f7ebdbf2fdff1bfa4c4b8376b4bbf=+; expires=Sun, 03-Nov-2024 09:42:02 GMT; Max-Age=0; path=/wordpress/
```

Request

```
GET /wordpress/ HTTP/1.1
Referer: http://192.168.1.5/
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: 192.168.1.5
Connection: Keep-alive
```

Recommendation

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

Cookies with missing, inconsistent or contradictory properties

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

CWE
CWE-284

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

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

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

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

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

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

Impact

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

http://192.168.1.5/ Verified

List of cookies with missing, inconsistent or contradictory properties:

- http://192.168.1.5/wordpress/

  Cookie was set with:

  ```
  Set-Cookie: PHPSESSID=nt36t21i6j2s3qvn17255ejgni; path=/
  ```

  This cookie has the following issues:

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

- http://192.168.1.5/wordpress/

  Cookie was set with:

  ```
  Set-Cookie: ec_cart_id=GBBQYPNKBUSYMSPGDLURKTQEGRKPQF; expires=Wed, 03-Dec-2025 09:13:10 GMT; Max-Age=2592000
  ```

  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://192.168.1.5/wordpress/xmlrpc.php

  Cookie was set with:

  ```
  Set-Cookie: PHPSESSID=24busvcfb909uhjt8582cmnvqc; path=/
  ```

  This cookie has the following issues:

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

- http://192.168.1.5/wordpress/xmlrpc.php

  Cookie was set with:

  ```
  Set-Cookie: ec_cart_id=KMLJISIMSIRGSUWKKGLAZRAGDKWMWD; expires=Wed, 03-Dec-2025 09:18:59 GMT; Max-Age=2592000
  ```

  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://192.168.1.5/wordpress/wp-comments-post.php

  Cookie was set with:

  ```
  Set-Cookie: comment_author_311f7ebdbf2fdff1bfa4c4b8376b4bbf=sOdPqaAH; expires=Fri, 16-Oct-2026 14:41:34 GMT; Max-Age=30000000;
  path=/wordpress/
  ```

  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://192.168.1.5/wordpress/wp-comments-post.php

  Cookie was set with:

  ```
  Set-Cookie: comment_author_email_311f7ebdbf2fdff1bfa4c4b8376b4bbf=testing%40example.com; expires=Fri, 16-Oct-2026 14:41:34 GMT;
  Max-Age=30000000; path=/wordpress/
  ```

  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://192.168.1.5/wordpress/wp-comments-post.php

  Cookie was set with:

  ```
  Set-Cookie: comment_author_url_311f7ebdbf2fdff1bfa4c4b8376b4bbf=http%3A%2F%2Fwww.example.com; expires=Fri, 16-Oct-2026 14:41:34
  GMT; Max-Age=30000000; path=/wordpress/
  ```

  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://192.168.1.5/wordpress/wp-login.php

  Cookie was set with:

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

  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://192.168.1.5/wordpress/wp-comments-post.php

  Cookie was set with:

  ```
  Set-Cookie: comment_author_311f7ebdbf2fdff1bfa4c4b8376b4bbf=1; expires=Fri, 16-Oct-2026 14:47:09 GMT; Max-Age=30000000;
  path=/wordpress/
  ```

  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://192.168.1.5/wordpress/wp-comments-post.php

  Cookie was set with:

  ```
  Set-Cookie: comment_author_email_311f7ebdbf2fdff1bfa4c4b8376b4bbf=testing%40example.com; expires=Fri, 16-Oct-2026 14:47:09 GMT;
  Max-Age=30000000; path=/wordpress/
  ```

  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://192.168.1.5/wordpress/wp-comments-post.php

  Cookie was set with:

  ```
  Set-Cookie: comment_author_url_311f7ebdbf2fdff1bfa4c4b8376b4bbf=http%3A%2F%2Fwww.example.com; expires=Fri, 16-Oct-2026 14:47:09
  GMT; Max-Age=30000000; path=/wordpress/
  ```

  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://192.168.1.5/wordpress/xmlrpc.php

  Cookie was set with:

  ```
  Set-Cookie: PHPSESSID=kdanbgpv3f2aml1tqh21g5vvru; path=/
  ```

  This cookie has the following issues:

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

- http://192.168.1.5/wordpress/xmlrpc.php

  Cookie was set with:

  ```
  Set-Cookie: ec_cart_id=QGVRJYGDZHYXZDLVJFJAKYNRGFPLFZ; expires=Wed, 03-Dec-2025 09:39:04 GMT; Max-Age=2592000
  ```

  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://192.168.1.5/wordpress/xmlrpc.php

  Cookie was set with:

  ```
  Set-Cookie: PHPSESSID=gefo47tpr1q5b188ct9qkrgalk; path=/
  ```

  This cookie has the following issues:

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

- http://192.168.1.5/wordpress/xmlrpc.php

  Cookie was set with:

  ```
  Set-Cookie: ec_cart_id=DAVMQAKFOICTWLBSDXESPLMOZXIDFS; expires=Wed, 03-Dec-2025 09:41:24 GMT; Max-Age=2592000
  ```

  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://192.168.1.5/wordpress/wp-login.php

  Cookie was set with:

  ```
  Set-Cookie: wordpress_311f7ebdbf2fdff1bfa4c4b8376b4bbf=+; expires=Sun, 03-Nov-2024 09:42:02 GMT; Max-Age=0; path=/wordpress/wp-
  admin
  ```

  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://192.168.1.5/wordpress/wp-login.php

  Cookie was set with:

  ```
  Set-Cookie: wordpress_sec_311f7ebdbf2fdff1bfa4c4b8376b4bbf=+; expires=Sun, 03-Nov-2024 09:42:02 GMT; Max-Age=0;
  path=/wordpress/wp-admin
  ```

  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://192.168.1.5/wordpress/wp-login.php

  Cookie was set with:

  ```
  Set-Cookie: wordpress_logged_in_311f7ebdbf2fdff1bfa4c4b8376b4bbf=+; expires=Sun, 03-Nov-2024 09:42:02 GMT; Max-Age=0;
  path=/wordpress/
  ```

  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://192.168.1.5/wordpress/wp-login.php

  Cookie was set with:

  ```
  Set-Cookie: wp-settings-0=+; expires=Sun, 03-Nov-2024 09:42:02 GMT; Max-Age=0; path=/wordpress/
  ```

  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://192.168.1.5/wordpress/wp-login.php

  Cookie was set with:

  ```
  Set-Cookie: wp-settings-time-0=+; expires=Sun, 03-Nov-2024 09:42:02 GMT; Max-Age=0; path=/wordpress/
  ```

  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://192.168.1.5/wordpress/wp-login.php

  Cookie was set with:

  ```
  Set-Cookie: wordpressuser_311f7ebdbf2fdff1bfa4c4b8376b4bbf=+; expires=Sun, 03-Nov-2024 09:42:02 GMT; Max-Age=0; path=/wordpress/
  ```

  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 /wordpress/ HTTP/1.1
Referer: http://192.168.1.5/
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: 192.168.1.5
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 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://192.168.1.5/wordpress/wp-login.php

Request

```
POST /wordpress//wp-login.php HTTP/1.1
Content-type: application/x-www-form-urlencoded
Cookie: ec_cart_id=GBBQYPNKBUSYMSPGDLURKTQEGRKPQF; PHPSESSID=nt36t21i6j2s3qvn17255ejgni
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: 192.168.1.5
Connection: Keep-alive

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

Recommendation

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

References

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

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

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

Content Security Policy (CSP) Not Implemented

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

Content Security Policy (CSP) can be implemented by adding a **Content-Security-Policy** header. The value of this header is a string containing the

policy directives describing your Content Security Policy. To implement CSP, you should define lists of allowed origins for the all of the types of resources that your site utilizes. For example, if you have a simple site that needs to load scripts, stylesheets, and images hosted locally, as well as from the jQuery library from their CDN, the CSP header could look like the following:

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

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

CWE
CWE-1021

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

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

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

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

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

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

Impact

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

http://192.168.1.5/

Paths without CSP header:

- http://192.168.1.5/
- http://192.168.1.5/manual
- http://192.168.1.5/wordpress/
- http://192.168.1.5/wordpress/readme.html
- http://192.168.1.5/wordpress/index.php/2019/09/09/hello-world/
- http://192.168.1.5/wordpress/wp-admin/images/
- http://192.168.1.5/wordpress/wp-admin/install.php
- http://192.168.1.5/wordpress/wp-includes/
- http://192.168.1.5/wordpress/wp-admin/upgrade.php
- http://192.168.1.5/wordpress/wp-login.php
- http://192.168.1.5/wordpress/wp-includes/ID3/
- http://192.168.1.5/wordpress/index.php/author/admin/
- http://192.168.1.5/wordpress/wp-includes/ID3/getid3.lib.php

- http://192.168.1.5/wordpress/index.php/category/uncategorized/

Request

```
GET / HTTP/1.1
Referer: http://192.168.1.5/
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: 192.168.1.5
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://192.168.1.5/

Request

```
GET /123ICWG1Dh 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: 192.168.1.5
```

```
Connection: Keep-alive
```

Recommendation

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

References

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

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

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

Permissions-Policy header not implemented

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

CWE
CWE-1021

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

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

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

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

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

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

Impact

http://192.168.1.5/

Locations without Permissions-Policy header:

- http://192.168.1.5/
- http://192.168.1.5/icons/
- http://192.168.1.5/manual
- http://192.168.1.5/wordpress/
- http://192.168.1.5/wordpress/readme.html
- http://192.168.1.5/wordpress/wp-content/plugins/wp-symposium/ajax/symposium_ajax_functions.php
- http://192.168.1.5/wordpress/wp-content/plugins/wp-symposium/ajax/symposium_mail_functions.php
- http://192.168.1.5/wordpress/index.php/2019/09/09/hello-world/
- http://192.168.1.5/wordpress/wp-comments-post.php
- http://192.168.1.5/wordpress/wp-login.php
- http://192.168.1.5/wordpress/wp-admin/images/
- http://192.168.1.5/wordpress/wp-admin/install.php
- http://192.168.1.5/wordpress/wp-includes/
- http://192.168.1.5/wordpress/wp-admin/upgrade.php
- http://192.168.1.5/wordpress/wp-includes/ID3/
- http://192.168.1.5/wordpress/index.php/author/admin/
- http://192.168.1.5/wordpress/wp-includes/ID3/getid3.lib.php

- http://192.168.1.5/wordpress/index.php/category/uncategorized/

Request

```
GET / HTTP/1.1
Referer: http://192.168.1.5/
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: 192.168.1.5
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/

Insecure HTTP Usage

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

CWE
CWE-16

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

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

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

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

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

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

Impact

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

http://192.168.1.5/

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: 192.168.1.5
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

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 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://192.168.1.5/wordpress/

wordpress v5.2.23-5.2.23

References

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

CKEditor Other Vulnerability

CKEditor4 is an open source what-you-see-is-what-you-get HTML editor. CKEditor4 prior to version 4.18.0 contains a vulnerability in the `dialog` plugin. The vulnerability allows abuse of a dialog input validator regular expression, which can cause a significant performance drop resulting in a browser tab freeze. A patch is available in version 4.18.0. There are currently no known workarounds.

CVSS3

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

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

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	None
Availability Impact	High

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://192.168.1.5/

ckeditor v4.5.4-4.5.4

References

CVE-2022-24729
https://nvd.nist.gov/vuln/detail/CVE-2022-24729

Gwolle Guestbook Cross-Site Scripting

WordPress Plugin Gwolle Guestbook is prone to a cross-site scripting vulnerability because it fails to properly sanitize user-supplied input. 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. This can allow the attacker to steal cookie-based authentication credentials and launch other attacks. WordPress Plugin Gwolle Guestbook version 2.5.3 is vulnerable; prior versions may also be affected.

CWE
CWE-79

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

Access Vector	Network
Access Complexity	Medium
Authentication	Single
Confidentiality	None
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: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/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	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://192.168.1.5/wordpress/wp-content/plugins/gwolle-gb/

gwolle-gb v1.5.3-1.5.3

Recommendation

Update to plugin version 2.5.4 or latest

References

http://www.defensecode.com/advisories/DC-2018-05-008_WordPress_Gwolle_Guestbook_Plugin_Advisory.pdf
http://www.defensecode.com/advisories/DC-2018-05-008_WordPress_Gwolle_Guestbook_Plugin_Advisory.pdf

https://packetstormsecurity.com/files/148715/WordPress-Gwolle-Guestbook-2.5.3-Cross-Site-Scripting.html
https://packetstormsecurity.com/files/148715/WordPress-Gwolle-Guestbook-2.5.3-Cross-Site-Scripting.html

https://plugins.svn.wordpress.org/gwolle-gb/trunk/readme.txt

https://plugins.svn.wordpress.org/gwolle-gb/trunk/readme.txt

Gwolle Guestbook Multiple Vulnerabilities

WordPress Plugin Gwolle Guestbook is prone to multiple vulnerabilities, including cross-site scripting and cross-site 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 and launch other attacks, or to perform certain administrative actions and gain unauthorized access to the affected application. WordPress Plugin Gwolle Guestbook version 2.1.0 is vulnerable; prior versions may also be affected.

CWE

CWE-352

CVSS2

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

Access Vector	Network
Access Complexity	Medium
Authentication	None
Confidentiality	None
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:N/I:L/A:N

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

CVSS4

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

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

Impact

http://192.168.1.5/wordpress/wp-content/plugins/gwolle-gb/

gwolle-gb v1.5.3-1.5.3

Recommendation

Update to plugin version 2.1.1 or latest

References

https://sumofpwn.nl/advisory/2016/gwolle_guestbook_mass_action_vulnerable_for_cross_site_request_forgery.html
https://sumofpwn.nl/advisory/2016/gwolle_guestbook_mass_action_vulnerable_for_cross_site_request_forgery.html

https://sumofpwn.nl/advisory/2016/cross_site_scripting_vulnerability_in_gwolle_guestbook_wordpress_plugin.html
https://sumofpwn.nl/advisory/2016/cross_site_scripting_vulnerability_in_gwolle_guestbook_wordpress_plugin.html

http://www.openwall.com/lists/oss-security/2017/03/01/4
http://www.openwall.com/lists/oss-security/2017/03/01/4

http://www.openwall.com/lists/oss-security/2017/03/01/3
http://www.openwall.com/lists/oss-security/2017/03/01/3

https://packetstormsecurity.com/files/141416/WordPress-Gwolle-Guestbook-1.7.4-Cross-Site-Request-Forgery.html
https://packetstormsecurity.com/files/141416/WordPress-Gwolle-Guestbook-1.7.4-Cross-Site-Request-Forgery.html

https://packetstormsecurity.com/files/141411/WordPress-Gwolle-Guestbook-1.7.4-Cross-Site-Scripting.html
https://packetstormsecurity.com/files/141411/WordPress-Gwolle-Guestbook-1.7.4-Cross-Site-Scripting.html

https://wordpress.org/plugins/gwolle-gb/changelog/
https://wordpress.org/plugins/gwolle-gb/changelog/

Gwolle Guestbook Remote File Inclusion

WordPress Plugin Gwolle Guestbook is prone to a remote file inclusion vulnerability because it fails to properly verify user-supplied input. An attacker can exploit this issue to include arbitrary remote files containing malicious PHP code and execute it in the context of the webserver process. This may

allow the attacker to compromise the application and to gain access to the underlying system. WordPress Plugin Gwolle Guestbook version 1.5.3 is vulnerable; prior versions may also be affected.

CWE
CWE-98

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

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

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

Base Score	9
Attack Vector	Network
Attack Complexity	High
Privileges Required	None
User Interaction	None
Scope	Changed
Confidentiality	High
Integrity Impact	High
Availability Impact	High

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

Base Score	9.2
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	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://192.168.1.5/wordpress/wp-content/plugins/gwolle-gb/

gwolle-gb v1.5.3-1.5.3

Recommendation

Update to plugin version 1.5.4 or latest

References

https://www.htbridge.com/advisory/HTB23275
https://www.htbridge.com/advisory/HTB23275

https://www.exploit-db.com/exploits/38861/
https://www.exploit-db.com/exploits/38861/

https://packetstormsecurity.com/files/134599/WordPress-Gwolle-Guestbook-1.5.3-Remote-File-Inclusion.html
https://packetstormsecurity.com/files/134599/WordPress-Gwolle-Guestbook-1.5.3-Remote-File-Inclusion.html

https://wordpress.org/plugins/gwolle-gb/changelog/
https://wordpress.org/plugins/gwolle-gb/changelog/

Mail Masta Local File Inclusion

WordPress Plugin Mail Masta is prone to a local file inclusion vulnerability because it fails to sufficiently verify user-supplied input. Exploiting this issue may allow an attacker to obtain sensitive information that could aid in further attacks. WordPress Plugin Mail Masta version 1.0 is vulnerable.

CWE
CWE-22

CVSS2
AV:N/AC:L/Au:N/C:P/I:N/A:N/E:POC/RL:U/RC:UR

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	None
Availability Impact	None
Exploitability	Proof of concept code

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

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

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

Remediation Level	Unavailable
Report Confidence	Uncorroborated

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

http://192.168.1.5/wordpress/wp-content/plugins/mail-masta/

mail-masta v1.0-1.0

Recommendation

Edit the source code to ensure that input is properly verified or disable the plugin until a fix is available

References

https://www.exploit-db.com/exploits/40290/
https://www.exploit-db.com/exploits/40290/

https://packetstormsecurity.com/files/138481/WordPress-Mail-Master-1.0-Local-File-Inclusion.html
https://packetstormsecurity.com/files/138481/WordPress-Mail-Master-1.0-Local-File-Inclusion.html

Mail Masta Multiple SQL Injection Vulnerabilities

WordPress Plugin Mail Masta is prone to multiple SQL injection vulnerabilities because it fails to sufficiently sanitize user-supplied data before using it in an SQL query. Exploiting these issues could allow an attacker to compromise the application, access or modify data, or exploit latent vulnerabilities in the underlying database. WordPress Plugin Mail Masta version 1.0 is vulnerable.

CWE
CWE-89

CVSS2
AV:N/AC:L/Au:N/C:P/I:P/A:P/E:POC/RL:U/RC:C

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

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

Base Score	8.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Changed
Confidentiality	Low
Integrity Impact	Low
Availability Impact	Low

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

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

Impact

http://192.168.1.5/wordpress/wp-content/plugins/mail-masta/

mail-masta v1.0-1.0

Recommendation

Edit the source code to ensure that input is properly sanitised or disable the plugin until a fix is available

References

https://github.com/hamkovic/Mail-Masta-Wordpress-Plugin-SQL-Injection-Vulnerability

https://github.com/hamkovic/Mail-Masta-Wordpress-Plugin-SQL-Injection-Vulnerability
https://www.exploit-db.com/exploits/41438/
https://www.exploit-db.com/exploits/41438/

https://packetstormsecurity.com/files/141277/WordPress-Mail-Masta-1.0-SQL-Injection.html
https://packetstormsecurity.com/files/141277/WordPress-Mail-Masta-1.0-SQL-Injection.html

ReFlex Gallery Arbitrary File Upload

WordPress Plugin ReFlex Gallery is prone to a vulnerability that lets attackers upload arbitrary files because the application fails to properly sanitize user-supplied input. An attacker can exploit this vulnerability to upload arbitrary code and run it in the context of the webserver process. This may facilitate unauthorized access or privilege escalation; other attacks are also possible. WordPress Plugin ReFlex Gallery version 3.1.3 is vulnerable; prior versions may also be affected.

CWE
CWE-434

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

Access Vector	Network
Access Complexity	Low
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:C/C:L/I:L/A:L

Base Score	8.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Changed
Confidentiality	Low
Integrity Impact	Low
Availability Impact	Low

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

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

Impact

http://192.168.1.5/wordpress/wp-content/plugins/reflex-gallery/
reflex-gallery v3.1.3-3.1.3

Recommendation

Update to plugin version 3.1.4 or latest

References

http://www.exploit-db.com/exploits/36374/
http://www.exploit-db.com/exploits/36374/

http://packetstormsecurity.com/files/130845/WordPress-Reflex-Gallery-3.1.3-Shell-Upload.html
http://packetstormsecurity.com/files/130845/WordPress-Reflex-Gallery-3.1.3-Shell-Upload.html

https://github.com/googleinurl/Wordpress-Plugin-Reflex-Gallery-Arbitrary-File-Upload
https://github.com/googleinurl/Wordpress-Plugin-Reflex-Gallery-Arbitrary-File-Upload

http://packetstormsecurity.com/files/131515/WordPress-Reflex-Gallery-Upload.html
http://packetstormsecurity.com/files/131515/WordPress-Reflex-Gallery-Upload.html

https://www.exploit-db.com/exploits/36809/
https://www.exploit-db.com/exploits/36809/

ReFlex Gallery Cross-Site Scripting

WordPress Plugin ReFlex Gallery is prone to a cross-site scripting vulnerability because it fails to properly sanitize user-supplied input. 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. This can allow the attacker

to steal cookie-based authentication credentials and launch other attacks. WordPress Plugin ReFlex Gallery version 3.1.4 is vulnerable; prior versions may also be affected.

CWE
CWE-79

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

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

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

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

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:P/VC:N/VI:L/VA:N/SC: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	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://192.168.1.5/wordpress/wp-content/plugins/reflex-gallery/

reflex-gallery v3.1.3-3.1.3

Recommendation

Update to plugin version 3.1.5 or latest

References

https://blog.anantshri.info/forgotten_disclosure_dom_xss_prettyphoto
https://blog.anantshri.info/forgotten_disclosure_dom_xss_prettyphoto

https://github.com/wpscanteam/wpscan/issues/818
https://github.com/wpscanteam/wpscan/issues/818

https://github.com/scaron/prettyphoto/issues/149
https://github.com/scaron/prettyphoto/issues/149

http://www.perucrack.net/2014/07/haciendo-un-xss-en-plugin-prettyphoto.html
http://www.perucrack.net/2014/07/haciendo-un-xss-en-plugin-prettyphoto.html

Shopping Cart & eCommerce Store Arbitrary File Upload

WordPress Plugin Shopping Cart & eCommerce Store is prone to a vulnerability that lets attackers upload arbitrary files because the application fails to properly sanitize user-supplied input. An attacker can exploit this vulnerability to upload arbitrary code and run it in the context of the webserver process. This may facilitate unauthorized access or privilege escalation; other attacks are also possible. WordPress Plugin Shopping Cart & eCommerce Store version 3.0.8 is vulnerable; prior versions may also be affected.

CWE
CWE-434

CVSS2
AV:N/AC:L/Au:S/C:C/I:C/A:N/E:F/RL:OF/RC:C

Access Vector	Network
Access Complexity	Low
Authentication	Single
Confidentiality	Complete
Integrity Impact	Complete

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

Base Score	9.1
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:H/VI:H/VA:N/SC:N/SI:

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

Availability Impact	None
Exploitability	Functional exploit exists
Remediation Level	Official Fix
Report Confidence	Confirmed

Scope	Unchanged
Confidentiality	High
Integrity Impact	High
Availability Impact	None

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://192.168.1.5/wordpress/wp-content/plugins/wp-easycart/

wp-easycart v3.0.4-3.0.4

Recommendation

Update to plugin version 3.0.9 or latest

References

http://security.szurek.pl/wordpress-shopping-cart-304-unrestricted-file-upload.html
http://security.szurek.pl/wordpress-shopping-cart-304-unrestricted-file-upload.html

http://www.exploit-db.com/exploits/35730/
http://www.exploit-db.com/exploits/35730/

http://packetstormsecurity.com/files/129875/WordPress-Shopping-Cart-3.0.4-Unrestricted-File-Upload.html
http://packetstormsecurity.com/files/129875/WordPress-Shopping-Cart-3.0.4-Unrestricted-File-Upload.html

http://www.exploit-db.com/exploits/36043/
http://www.exploit-db.com/exploits/36043/

http://packetstormsecurity.com/files/130328/WordPress-WP-EasyCart-Unrestricted-File-Upload.html
http://packetstormsecurity.com/files/130328/WordPress-WP-EasyCart-Unrestricted-File-Upload.html

Shopping Cart & eCommerce Store Cross-Site Request Forgery

WordPress Plugin Shopping Cart & eCommerce Store 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 Plugin Shopping Cart & eCommerce Store version 5.1.0 is vulnerable; prior versions may also be affected.

CWE

CWE-352

CVSS2

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

Access Vector	Network
Access Complexity	Medium
Authentication	None
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: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

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://192.168.1.5/wordpress/wp-content/plugins/wp-easycart/

wp-easycart v3.0.4-3.0.4

Recommendation

Update to the latest plugin version

References

https://www.wordfence.com/vulnerability-advisories/#CVE-2021-34645
https://www.wordfence.com/vulnerability-advisories/#CVE-2021-34645

https://plugins.svn.wordpress.org/wp-easycart/trunk/readme.txt
https://plugins.svn.wordpress.org/wp-easycart/trunk/readme.txt

Shopping Cart & eCommerce Store Multiple Security Bypass Vulnerabilities

WordPress Plugin Shopping Cart & eCommerce Store is prone to multiple security bypass vulnerabilities. Exploiting these issues may allow attackers to perform otherwise restricted actions and subsequently update any WordPress options. WordPress Plugin Shopping Cart & eCommerce Store version 3.0.20 is vulnerable; prior versions may also be affected.

CWE
CWE-264

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://192.168.1.5/wordpress/wp-content/plugins/wp-easycart/

wp-easycart v3.0.4-3.0.4

Recommendation

Update to plugin version 3.0.22 or latest

References

https://www.rastating.com/wp-easycart-privilege-escalation-information-disclosure/
https://www.rastating.com/wp-easycart-privilege-escalation-information-disclosure/

https://github.com/rapid7/metasploit-framework/blob/master/modules/auxiliary/admin/http/wp_easycart_privilege_escalation.rb
https://github.com/rapid7/metasploit-framework/blob/master/modules/auxiliary/admin/http/wp_easycart_privilege_escalation.rb

Shopping Cart & eCommerce Store Unspecified Vulnerability

WordPress Plugin Shopping Cart & eCommerce Store is prone to an unspecified vulnerability. No available information exists regarding this issue and it's impact on a vulnerable website. WordPress Plugin Shopping Cart & eCommerce Store version 3.1.9 is vulnerable; prior versions may also be affected.

Impact

http://192.168.1.5/wordpress/wp-content/plugins/wp-easycart/

wp-easycart v3.0.4-3.0.4

Recommendation

Update to plugin version 3.1.10 or latest

References

https://wordpress.org/plugins/wp-easycart/changelog/
https://wordpress.org/plugins/wp-easycart/changelog/

Site Editor-WordPress Site Builder-Theme Builder and Page Builder Local File Inclusion

WordPress Plugin Site Editor-WordPress Site Builder-Theme Builder and Page Builder is prone to a local file inclusion vulnerability because it fails to sufficiently verify user-supplied input. Exploiting this issue may allow an attacker to obtain sensitive information that could aid in further attacks. WordPress Plugin Site Editor-WordPress Site Builder-Theme Builder and Page Builder version 1.1.1 is vulnerable; prior versions may also be affected.

CWE
CWE-22

CVSS2
AV:N/AC:L/Au:N/C:P/I:N/A:N/E:POC/RL:U/RC:C

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

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

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

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

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

http://192.168.1.5/wordpress/wp-content/plugins/site-editor/

site-editor v1.1.1-1.1.1

Recommendation

Edit the source code to ensure that input is properly verified or disable the plugin until a fix is available

References

http://seclists.org/fulldisclosure/2018/Mar/40
http://seclists.org/fulldisclosure/2018/Mar/40

https://www.exploit-db.com/exploits/44340/
https://www.exploit-db.com/exploits/44340/

https://packetstormsecurity.com/files/146796/WordPress-Site-Editor-1.1.1-Local-File-Inclusion.html
https://packetstormsecurity.com/files/146796/WordPress-Site-Editor-1.1.1-Local-File-Inclusion.html

Slideshow Gallery LITE Arbitrary File Upload

WordPress Plugin Slideshow Gallery LITE is prone to a vulnerability that lets attackers upload arbitrary files. The issue occurs because the application fails to adequately sanitize user-supplied input. An attacker can exploit this vulnerability to upload arbitrary code and run it in the context of the webserver process. This may facilitate unauthorized access or privilege escalation; other attacks are also possible. WordPress Plugin Slideshow Gallery LITE version 1.4.6 is vulnerable; prior versions may also be affected.

CWE
CWE-20

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

Access Vector	Network
Access Complexity	Low
Authentication	Single
Confidentiality	Partial
Integrity Impact	Partial
Availability Impact	Partial
Exploitability	Functional exploit exists
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/SA

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://192.168.1.5/wordpress/wp-content/plugins/slideshow-gallery/

slideshow-gallery v1.4.6-1.4.6

Recommendation

Update to plugin version 1.4.7 or latest

References

http://whitexploit.blogspot.mx/2014/08/wordpress-slideshow-gallery-146-shell.html
http://whitexploit.blogspot.mx/2014/08/wordpress-slideshow-gallery-146-shell.html

http://www.exploit-db.com/exploits/34514/
http://www.exploit-db.com/exploits/34514/

http://www.exploit-db.com/exploits/34681/
http://www.exploit-db.com/exploits/34681/

http://packetstormsecurity.com/files/128069/WordPress-Slideshow-Gallery-1.4.6-Shell-Upload.html
http://packetstormsecurity.com/files/128069/WordPress-Slideshow-Gallery-1.4.6-Shell-Upload.html

http://packetstormsecurity.com/files/131526/WordPress-SlideShow-Gallery-Authenticated-File-Upload.html
http://packetstormsecurity.com/files/131526/WordPress-SlideShow-Gallery-Authenticated-File-Upload.html

http://secunia.com/advisories/60074/
http://secunia.com/advisories/60074/

Slideshow Gallery LITE Cross-Site Scripting

WordPress Plugin Slideshow Gallery LITE is prone to a cross-site scripting vulnerability because it fails to properly sanitize user-supplied input. 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. This can allow the attacker to steal cookie-based authentication credentials and launch other attacks. WordPress Plugin Slideshow Gallery LITE version 1.5.3.4 is vulnerable; prior versions may also be affected.

CWE
CWE-79

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

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

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

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

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

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://192.168.1.5/wordpress/wp-content/plugins/slideshow-gallery/

slideshow-gallery v1.4.6-1.4.6

http://192.168.1.5/wordpress/wp-content/plugins/slideshow-gallery/

slideshow-gallery v1.4.6-1.4.6

http://192.168.1.5/wordpress/wp-content/plugins/slideshow-gallery/

slideshow-gallery v1.4.6-1.4.6

Recommendation

Update to plugin version 1.6.1 or latest

References

http://security.szurek.pl/tribulant-slideshow-gallery-1534-reflected-xss.html
http://security.szurek.pl/tribulant-slideshow-gallery-1534-reflected-xss.html

https://wordpress.org/plugins/slideshow-gallery/changelog/
https://wordpress.org/plugins/slideshow-gallery/changelog/

Slideshow Gallery LITE Multiple Cross-Site Scripting Vulnerabilities

WordPress Plugin Slideshow Gallery LITE is prone to multiple cross-site scripting vulnerabilities because it fails to properly sanitize user-supplied input. 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. This can allow the attacker to steal cookie-based authentication credentials and launch other attacks. WordPress Plugin Slideshow Gallery LITE version 1.6.5 is vulnerable; prior versions may also be affected.

CWE
CWE-79

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

Access Vector	Network
Access Complexity	Medium
Authentication	Single
Confidentiality	None
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: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/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	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://192.168.1.5/wordpress/wp-content/plugins/slideshow-gallery/

slideshow-gallery v1.4.6-1.4.6

Recommendation

Update to plugin version 1.6.6.1 or latest

References

http://www.defensecode.com/advisories/DC-2017-01-014_WordPress_Tribulant_Slideshow_Gallery_Plugin_Advisory.pdf
http://www.defensecode.com/advisories/DC-2017-01-014_WordPress_Tribulant_Slideshow_Gallery_Plugin_Advisory.pdf

https://packetstormsecurity.com/files/142079/WordPress-Tribulant-Slideshow-Gallery-1.6.5-Cross-Site-Scripting.html
https://packetstormsecurity.com/files/142079/WordPress-Tribulant-Slideshow-Gallery-1.6.5-Cross-Site-Scripting.html

https://wordpress.org/plugins/slideshow-gallery/#changelog
https://wordpress.org/plugins/slideshow-gallery/#changelog

Slideshow Gallery LITE Multiple Unspecified Vulnerabilities

WordPress Plugin Slideshow Gallery LITE is prone to multiple unspecified vulnerabilities. No available information exists regarding these issues and their impact on a vulnerable website. WordPress Plugin Slideshow Gallery LITE version 1.5.3.3 is vulnerable; prior versions may also be affected.

Impact

http://192.168.1.5/wordpress/wp-content/plugins/slideshow-gallery/

slideshow-gallery v1.4.6-1.4.6

Recommendation

Update to plugin version 1.5.3.4 or latest

References

https://wordpress.org/plugins/slideshow-gallery/changelog/
https://wordpress.org/plugins/slideshow-gallery/changelog/

Slideshow Gallery LITE Multiple Vulnerabilities

WordPress Plugin Slideshow Gallery LITE is prone to multiple vulnerabilities, including cross-site scripting and SQL injection vulnerabilities. Exploiting these issues could allow an attacker to execute arbitrary script code in the browser of an unsuspecting user in the context of the affected site, allowing the attacker to steal cookie-based authentication credentials, or to compromise the application, access or modify data, or exploit latent vulnerabilities in the underlying database. WordPress Plugin Slideshow Gallery LITE version 1.6.8 is vulnerable; prior versions may also be affected.

CWE
CWE-89

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

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

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

Base Score	7.1
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	Required
Scope	Changed

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

Base Score	5.1
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	Active

Exploitability	High
Remediation Level	Official Fix
Report Confidence	Confirmed

Confidentiality	Low
Integrity Impact	Low
Availability Impact	Low

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://192.168.1.5/wordpress/wp-content/plugins/slideshow-gallery/

slideshow-gallery v1.4.6-1.4.6

http://192.168.1.5/wordpress/wp-content/plugins/slideshow-gallery/

slideshow-gallery v1.4.6-1.4.6

http://192.168.1.5/wordpress/wp-content/plugins/slideshow-gallery/

slideshow-gallery v1.4.6-1.4.6

Recommendation

Update to plugin version 1.6.9 or latest

References

https://plugins.svn.wordpress.org/slideshow-gallery/trunk/readme.txt
https://plugins.svn.wordpress.org/slideshow-gallery/trunk/readme.txt

Slideshow Gallery LITE Unspecified Vulnerability

WordPress Plugin Slideshow Gallery LITE is prone to an unspecified vulnerability. No available information exists regarding this issue and it's impact on a vulnerable website. WordPress Plugin Slideshow Gallery LITE version 1.7.4.2 is vulnerable; prior versions may also be affected.

Impact

http://192.168.1.5/wordpress/wp-content/plugins/slideshow-gallery/

slideshow-gallery v1.4.6-1.4.6

http://192.168.1.5/wordpress/wp-content/plugins/slideshow-gallery/

slideshow-gallery v1.4.6-1.4.6

Recommendation

Update to plugin version 1.7.4.3 or latest

References

https://plugins.svn.wordpress.org/slideshow-gallery/trunk/readme.txt
https://plugins.svn.wordpress.org/slideshow-gallery/trunk/readme.txt

Underscore.js Improper Control of Generation of Code ('Code Injection') Vulnerability

The package underscore from 1.13.0-0 and before 1.13.0-2, from 1.3.2 and before 1.12.1 are vulnerable to Arbitrary Code Injection via the template function, particularly when a variable property is passed as an argument as it is not sanitized.

CWE
CWE-94

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

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

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://192.168.1.5/

underscore.js v1.8.3-1.8.3

References

CVE-2021-23358
https://nvd.nist.gov/vuln/detail/CVE-2021-23358

WordPress Deserialization of Untrusted Data Vulnerability

WordPress is a free and open-source content management system written in PHP and paired with a MariaDB database. On a multisite, users with Super Admin role can bypass explicit/additional hardening under certain conditions through object injection. This has been patched in WordPress version 5.8.3. Older affected versions are also fixed via security release, that go back till 3.7.37. We strongly recommend that you keep auto-updates enabled. There are no known workarounds for this issue.

CWE
CWE-502

CVSS3
CVSS:3.1/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://192.168.1.5/wordpress/

wordpress v5.2.23-5.2.23

References

CVE-2022-21663
https://nvd.nist.gov/vuln/detail/CVE-2022-21663

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://192.168.1.5/wordpress/
wordpress v5.2.23-5.2.23

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

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

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

WP Support Plus Responsive Ticket System Cross-Site Scripting

WordPress Plugin WP Support Plus Responsive Ticket System is prone to a cross-site scripting vulnerability because it fails to properly sanitize user-supplied input. 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. This can allow the attacker to steal cookie-based authentication credentials and launch other attacks. WordPress Plugin WP Support Plus Responsive Ticket System version 9.1.1 is vulnerable; prior versions may also be affected.

CWE
CWE-79

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

Access Vector	Network
Access Complexity	Medium
Authentication	None
Confidentiality	None

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

Base Score	4.7
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:L/VA:N/SC:N/

Base Score	5.1
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None

Integrity Impact	Partial
Availability Impact	None
Exploitability	Proof of concept code
Remediation Level	Official Fix
Report Confidence	Confirmed

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

Privileges Required	None
User Interaction	Active
Confidentiality Impact to the Vulnerable System	None
Integrity Impact to the Vulnerable System	Low
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

http://192.168.1.5/wordpress/wp-content/plugins/wp-support-plus-responsive-ticket-system/

wp-support-plus-responsive-ticket-system v7.1.3-7.1.3

Recommendation

Update to plugin version 9.1.2 or latest

References

https://cert.kalasag.com.ph/news/research/cve-2019-7299-stored-xss-in-wp-support-plus-responsive-ticket-system/
https://cert.kalasag.com.ph/news/research/cve-2019-7299-stored-xss-in-wp-support-plus-responsive-ticket-system/

https://plugins.svn.wordpress.org/wp-support-plus-responsive-ticket-system/trunk/readme.txt
https://plugins.svn.wordpress.org/wp-support-plus-responsive-ticket-system/trunk/readme.txt

WP Support Plus Responsive Ticket System PHP Object Injection

WordPress Plugin WP Support Plus Responsive Ticket System 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 Plugin WP Support Plus Responsive Ticket System version 9.0.3 is vulnerable; prior versions may also be affected.

CWE
CWE-915

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

Access Vector	Network
Access Complexity	Low
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:C/C:L/I:L/A:L

Base Score	8.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Changed
Confidentiality	Low
Integrity Impact	Low
Availability Impact	Low

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

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

Impact

http://192.168.1.5/wordpress/wp-content/plugins/wp-support-plus-responsive-ticket-system/

wp-support-plus-responsive-ticket-system v7.1.3-7.1.3

Recommendation

Update to plugin version 9.0.4 or latest

References

https://www.pluginvulnerabilities.com/2018/02/16/our-proactive-monitoring-caught-a-php-object-injection-vulnerability-in-a-fairly-popular-plugin/
https://www.pluginvulnerabilities.com/2018/02/16/our-proactive-monitoring-caught-a-php-object-injection-vulnerability-in-a-fairly-popular-plugin/

WP Support Plus Responsive Ticket System Privilege Escalation

WordPress Plugin WP Support Plus Responsive Ticket System is prone to a privilege escalation vulnerability. Exploiting this issue may allow attackers to bypass the expected capabilities check and perform otherwise restricted actions; other attacks are also possible. WordPress Plugin WP Support Plus Responsive Ticket System version 7.1.4 is vulnerable; prior versions may also be affected.

CWE
CWE-264

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

Access Vector	Network
Access Complexity	Low
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:L/I:L/A:L

Base Score	7.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity Impact	Low
Availability Impact	Low

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

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

Impact

http://192.168.1.5/wordpress/wp-content/plugins/wp-support-plus-responsive-ticket-system/

wp-support-plus-responsive-ticket-system v7.1.3-7.1.3

Recommendation

Update to plugin version 8.0.0 or latest

References

http://security.szurek.pl/wp-support-plus-responsive-ticket-system-713-privilege-escalation.html
http://security.szurek.pl/wp-support-plus-responsive-ticket-system-713-privilege-escalation.html

https://www.exploit-db.com/exploits/41006/
https://www.exploit-db.com/exploits/41006/

https://packetstormsecurity.com/files/140413/WordPress-WP-Support-Plus-Responsive-Ticket-System-7.1.3-Privilege-Escalation.html
https://packetstormsecurity.com/files/140413/WordPress-WP-Support-Plus-Responsive-Ticket-System-7.1.3-Privilege-Escalation.html

WP Support Plus Responsive Ticket System Security Bypass

WordPress Plugin WP Support Plus Responsive Ticket System is prone to a security bypass vulnerability. Exploiting this issue may allow attackers to perform otherwise restricted actions and subsequently login as any user without knowing the password. WordPress Plugin WP Support Plus Responsive Ticket System version 7.1.4 is vulnerable; prior versions may also be affected.

CWE
CWE-287

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

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

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

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

Base Score	7.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity Impact	Low
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	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://192.168.1.5/wordpress/wp-content/plugins/wp-support-plus-responsive-ticket-system/

wp-support-plus-responsive-ticket-system v7.1.3-7.1.3

Recommendation

Update to plugin version 8.0.0 or latest

References

https://security.szurek.pl/wp-support-plus-responsive-ticket-system-713-privilege-escalation.html
https://security.szurek.pl/wp-support-plus-responsive-ticket-system-713-privilege-escalation.html

https://plugins.svn.wordpress.org/wp-support-plus-responsive-ticket-system/trunk/readme.txt
https://plugins.svn.wordpress.org/wp-support-plus-responsive-ticket-system/trunk/readme.txt

WP Support Plus Responsive Ticket System SQL Injection

WordPress Plugin WP Support Plus Responsive Ticket System is prone to an SQL injection vulnerability because it fails to sufficiently sanitize user-supplied data before using it in an SQL query. Exploiting this issue could allow an attacker to compromise the application, access or modify data, or exploit latent vulnerabilities in the underlying database. WordPress Plugin WP Support Plus Responsive Ticket System version 7.1.4 is vulnerable; prior versions may also be affected.

CWE

CWE-89

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://192.168.1.5/wordpress/wp-content/plugins/wp-support-plus-responsive-ticket-system/

wp-support-plus-responsive-ticket-system v7.1.3-7.1.3

Recommendation

Update to plugin version 7.1.5 or latest

References

http://lenonleite.com.br/en/blog/2016/12/13/wp-support-plus-responsive-ticket-system-wordpress-plugin-sql-injection/
http://lenonleite.com.br/en/blog/2016/12/13/wp-support-plus-responsive-ticket-system-wordpress-plugin-sql-injection/

https://www.exploit-db.com/exploits/40939/
https://www.exploit-db.com/exploits/40939/

https://packetstormsecurity.com/files/140203/WordPress-Support-Plus-Responsive-Ticket-System-7.1.3-SQL-Injection.html
https://packetstormsecurity.com/files/140203/WordPress-Support-Plus-Responsive-Ticket-System-7.1.3-SQL-Injection.html

https://wordpress.org/plugins/wp-support-plus-responsive-ticket-system/changelog/
https://wordpress.org/plugins/wp-support-plus-responsive-ticket-system/changelog/

WP Support Plus Responsive Ticket System Unspecified Vulnerability

WordPress Plugin WP Support Plus Responsive Ticket System is prone to an unspecified vulnerability. No available information exists regarding this issue and it's impact on a vulnerable website. WordPress Plugin WP Support Plus Responsive Ticket System version 8.0.7 is vulnerable; prior versions may also be affected.

Impact

http://192.168.1.5/wordpress/wp-content/plugins/wp-support-plus-responsive-ticket-system/

wp-support-plus-responsive-ticket-system v7.1.3-7.1.3

Recommendation

Update to plugin version 8.0.8 or latest

References

https://plugins.svn.wordpress.org/wp-support-plus-responsive-ticket-system/trunk/readme.txt
https://plugins.svn.wordpress.org/wp-support-plus-responsive-ticket-system/trunk/readme.txt

WP Symposium Cross-Site Scripting

WordPress Plugin WP Symposium is prone to a cross-site scripting vulnerability because it fails to properly sanitize user-supplied input. 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. This can allow the attacker to steal cookie-based authentication credentials and launch other attacks. WordPress Plugin WP Symposium version 15.8.1 is vulnerable; prior versions may also be affected.

CWE
CWE-79

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

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

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

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

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:P/VC:N/VI:L/VA:N/SC: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	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://192.168.1.5/wordpress/wp-content/plugins/wp-symposium/

wp-symposium v15.1-15.1

Recommendation

Edit the source code to ensure that input is properly sanitised or disable the plugin until a fix is available

References

http://cxsecurity.com/issue/WLB-2015090024
http://cxsecurity.com/issue/WLB-2015090024

WP Symposium SQL Injection

WordPress Plugin WP Symposium is prone to an SQL injection vulnerability because it fails to sufficiently sanitize user-supplied data before using it in an SQL query. Exploiting this issue could allow an attacker to compromise the application, access or modify data, or exploit latent vulnerabilities in the underlying database. WordPress Plugin WP Symposium version 15.5.1 is vulnerable; prior versions may also be affected.

CWE
CWE-89

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

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

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

Base Score	10
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Changed
Confidentiality	High
Integrity Impact	High
Availability Impact	None

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:N/SC: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	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

http://192.168.1.5/wordpress/wp-content/plugins/wp-symposium/

wp-symposium v15.1-15.1

http://192.168.1.5/wordpress/wp-content/plugins/wp-symposium/

wp-symposium v15.1-15.1

Recommendation

Update to plugin version 15.8 or latest

References

https://security.dxw.com/advisories/blind-sql-injection-in-wp-symposium-allows-unauthenticated-attackers-to-access-sensitive-data/
https://security.dxw.com/advisories/blind-sql-injection-in-wp-symposium-allows-unauthenticated-attackers-to-access-sensitive-data/

https://www.exploit-db.com/exploits/37822/
https://www.exploit-db.com/exploits/37822/

https://packetstormsecurity.com/files/133047/WordPress-WP-Symposium-15.1-SQL-Injection.html
https://packetstormsecurity.com/files/133047/WordPress-WP-Symposium-15.1-SQL-Injection.html

https://www.exploit-db.com/exploits/37824/
https://www.exploit-db.com/exploits/37824/

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

CKEditor4 is an open source what-you-see-is-what-you-get HTML editor. A cross-site scripting vulnerability has been discovered affecting Iframe Dialog and Media Embed packages. The vulnerability may trigger a JavaScript code after fulfilling special conditions: using one of the affected packages on a web page with missing proper Content Security Policy configuration; initializing the editor on an element and using an element other than `<textarea>` as a base; and destroying the editor instance. This vulnerability might affect a small percentage of integrators that depend on dynamic editor initialization/destroy mechanism. A fix is available in CKEditor4 version 4.21.0. In some rare cases, a security fix may be considered a breaking change. Starting from version 4.21.0, the Iframe Dialog plugin applies the `sandbox` attribute by default, which restricts JavaScript code execution in the iframe element. To change this behavior, configure the `config.iframe_attributes` option. Also starting from version 4.21.0, the Media Embed plugin regenerates the entire content of the embed widget by default. To change this behavior, configure the `config.embed_keepOriginalContent` option. Those who choose to enable either of the more permissive options or who cannot upgrade to a patched version should properly configure Content Security Policy to avoid any potential security issues that may arise from embedding iframe elements on their web page.

CWE
CWE-707

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

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

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

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

Impact

http://192.168.1.5/
ckeditor v4.5.4-4.5.4

http://192.168.1.5/
ckeditor v4.5.4-4.5.4

http://192.168.1.5/
ckeditor v4.5.4-4.5.4

http://192.168.1.5/
ckeditor v4.5.4-4.5.4

http://192.168.1.5/
ckeditor v4.5.4-4.5.4

http://192.168.1.5/
ckeditor v4.5.4-4.5.4

http://192.168.1.5/

ckeditor v4.5.4-4.5.4

References

CVE-2023-28439
https://nvd.nist.gov/vuln/detail/CVE-2023-28439

CKEditor Inclusion of Functionality from Untrusted Control Sphere Vulnerability

It was possible to execute a ReDoS-type attack inside CKEditor 4 before 4.16 by persuading a victim to paste crafted text into the Styles input of specific dialogs (in the Advanced Tab for Dialogs plugin).

CWE
CWE-829

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

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

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

Base Score	6.9
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	High
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

http://192.168.1.5/

ckeditor v4.5.4-4.5.4

http://192.168.1.5/

ckeditor v4.5.4-4.5.4

References

CVE-2021-26271
https://nvd.nist.gov/vuln/detail/CVE-2021-26271

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

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

CWE
CWE-707

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

Base Score	6.1
Attack Vector	Network
Attack Complexity	Low

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

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

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://192.168.1.5/

jquery v1.12.4-1.12.4

http://192.168.1.5/

jquery v1.12.4-1.12.4

http://192.168.1.5/

jquery v1.12.4-1.12.4

References

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

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

prettyPhoto before 3.1.6 has js/jquery.prettyPhoto.js XSS.

CWE
CWE-707

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

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

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

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

Impact

http://192.168.1.5/

jquery.prettyphoto v3.1.5-3.1.5

References

CVE-2015-9478
https://nvd.nist.gov/vuln/detail/CVE-2015-9478

JQuery Prototype Pollution Vulnerability

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

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

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

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

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

Impact

http://192.168.1.5/
jquery v1.12.4-1.12.4

References

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

JQuery UI Cross-site Scripting (XSS) Vulnerability

Cross-site scripting (XSS) vulnerability in jQuery UI before 1.12.0 might allow remote attackers to inject arbitrary web script or HTML via the closeText parameter of the dialog function.

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

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

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

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

Availability Impact to the Subsequent System	None

Impact

http://192.168.1.5/

jquery-ui-dialog v1.11.4-1.11.4

http://192.168.1.5/

jquery-ui-tooltip v1.10.3-1.10.3

References

CVE-2016-7103
https://nvd.nist.gov/vuln/detail/CVE-2016-7103

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

jQuery-UI is the official jQuery user interface library. Prior to version 1.13.0, accepting the value of various `*Text` options of the Datepicker widget from untrusted sources may execute untrusted code. The issue is fixed in jQuery UI 1.13.0. The values passed to various `*Text` options are now always treated as pure text, not HTML. A workaround is to not accept the value of the `*Text` options from untrusted sources.

CWE

CWE-707

CVSS3

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

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

CVSS4

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

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

Impact

http://192.168.1.5/

jquery-ui-dialog v1.11.4-1.11.4

http://192.168.1.5/

jquery-ui-dialog v1.11.4-1.11.4

http://192.168.1.5/

jquery-ui-dialog v1.11.4-1.11.4

References

CVE-2021-41183
https://nvd.nist.gov/vuln/detail/CVE-2021-41183

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

jQuery-UI is the official jQuery user interface library. Prior to version 1.13.0, accepting the value of the `of` option of the `.position()` util from untrusted sources may execute untrusted code. The issue is fixed in jQuery UI 1.13.0. Any string value passed to the `of` option is now treated as a CSS selector. A workaround is to not accept the value of the `of` option from untrusted sources.

CWE
CWE-707

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

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

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

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

Impact

http://192.168.1.5/
jquery-ui-tooltip v1.10.3-1.10.3

http://192.168.1.5/
jquery-ui-tooltip v1.10.3-1.10.3

http://192.168.1.5/
jquery-ui-tooltip v1.10.3-1.10.3

References

CVE-2021-41184
https://nvd.nist.gov/vuln/detail/CVE-2021-41184

Vulnerable JavaScript libraries

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

CWE
CWE-937

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

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

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

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

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

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

Availability Impact	None

Integrity Impact	Low
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

Consult References for more information.

http://192.168.1.5/ Confidence: 95%

- jQuery 1.12.4
  - URL: http://192.168.1.5/wordpress/
  - Detection method: The library's name and version were determined based on its dynamic behavior.
  - CVE-ID: CVE-2015-9251, CVE-2020-11022, CVE-2020-11023
  - Description: Possible Cross Site Scripting via third-party text/javascript responses (1.12.0-1.12.2 mitigation reverted) / In jQuery versions greater than or equal to 1.2 and before 3.5.0, passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0. / In jQuery versions greater than or equal to 1.0.3 and before 3.5.0, passing HTML containing option elements from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.
  - References:
    - https://github.com/jquery/jquery/issues/2432
    - https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/
    - https://mksben.l0.cm/2020/05/jquery3.5.0-xss.html
    - https://jquery.com/upgrade-guide/3.5/
    - https://api.jquery.com/jQuery.htmlPrefilter/
    - https://www.cvedetails.com/cve/CVE-2020-11022/
    - https://github.com/advisories/GHSA-gxr4-xjj5-5px2
    - https://www.cvedetails.com/cve/CVE-2020-11023/
    - https://github.com/advisories/GHSA-jpcq-cgw6-v4j6

Request

```
GET /wordpress/ HTTP/1.1
Referer: http://192.168.1.5/
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: 192.168.1.5
Connection: Keep-alive
```

http://192.168.1.5/ Confidence: 95%

- jQuery UI Dialog 1.11.4
  - URL: http://192.168.1.5/wordpress/
  - Detection method: The library's name and version were determined based on its dynamic behavior.
  - CVE-ID: CVE-2016-7103
  - Description: XSS in dialog closeText
  - References:
    - https://nodesecurity.io/advisories/127
    - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7103
    - https://www.cvedetails.com/cve/CVE-2016-7103/

Request

```
GET /wordpress/ HTTP/1.1
Referer: http://192.168.1.5/
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: 192.168.1.5
Connection: Keep-alive
```

http://192.168.1.5/ Confidence: 95%

- jQuery UI Datepicker 1.11.4
  - URL: http://192.168.1.5/wordpress/
  - Detection method: The library's name and version were determined based on its dynamic behavior.
  - CVE-ID: CVE-2021-41182, CVE-2021-41183
  - Description: XSS in the 'altField' option of the Datepicker widget / XSS in '*Text' options of the Datepicker widget
  - References:
    - https://blog.jqueryui.com/2021/10/jquery-ui-1-13-0-released/
    - https://github.com/jquery/jquery-ui/security/advisories/GHSA-9gj3-hwp5-pmwc
    - https://github.com/jquery/jquery-ui/security/advisories/GHSA-j7qv-pgf6-hvh4

Request

```
GET /wordpress/ HTTP/1.1
Referer: http://192.168.1.5/
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: 192.168.1.5
Connection: Keep-alive
```

http://192.168.1.5/ Confidence: 95%

- jQuery prettyPhoto 3.1.5
  - URL: http://192.168.1.5/wordpress/
  - Detection method: The library's name and version were determined based on its dynamic behavior.
  - CVE-ID: N/A
  - Description: DOM XSS
  - References:
    - https://github.com/scaron/prettyphoto/issues/149
    - https://blog.anantshri.info/forgotten_disclosure_dom_xss_prettyphoto

Request

```
GET /wordpress/ HTTP/1.1
Referer: http://192.168.1.5/
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: 192.168.1.5
Connection: Keep-alive
```

http://192.168.1.5/ Confidence: 95%

- jQuery UI Dialog 1.10.3
  - URL: http://192.168.1.5/wordpress/wp-login.php
  - Detection method: The library's name and version were determined based on its dynamic behavior.
  - CVE-ID: CVE-2016-7103
  - Description: XSS in dialog closeText
  - References:
    - https://nodesecurity.io/advisories/127
    - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7103
    - https://www.cvedetails.com/cve/CVE-2016-7103/

Request

```
POST /wordpress/wp-login.php HTTP/1.1
Referer: http://192.168.1.5/wordpress/
Cookie: comment_author_311f7ebdbf2fdff1bfa4c4b8376b4bbf=sOdPqaAH; comment_author_email_311f7ebdbf2fdff1bfa4c4b8376b4bbf=testing%40example.com;
comment_author_url_311f7ebdbf2fdff1bfa4c4b8376b4bbf=http%3A%2F%2Fwww.example.com; wordpress_test_cookie=WP+Cookie+check;
ec_cart_id=KRZULVEOJJCQRXPJOVCUNFMMHEFDBE; PHPSESSID=aqceka9dkvqmo63rrm46ru828b
Content-Type: application/x-www-form-urlencoded
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Content-Length: 41
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: 192.168.1.5
Connection: Keep-alive

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

http://192.168.1.5/ Confidence: 95%

- **jQuery UI Datepicker 1.10.3**
  - URL: http://192.168.1.5/wordpress/wp-login.php
  - Detection method: The library's name and version were determined based on its dynamic behavior.
  - CVE-ID: CVE-2021-41182, CVE-2021-41183
  - Description: XSS in the 'altField' option of the Datepicker widget / XSS in '*Text' options of the Datepicker widget
  - References:
    - https://blog.jqueryui.com/2021/10/jquery-ui-1-13-0-released/
    - https://github.com/jquery/jquery-ui/security/advisories/GHSA-9gj3-hwp5-pmwc
    - https://github.com/jquery/jquery-ui/security/advisories/GHSA-j7qv-pgf6-hvh4

Request

```
POST /wordpress/wp-login.php HTTP/1.1
Referer: http://192.168.1.5/wordpress/
Cookie: comment_author_311f7ebdbf2fdff1bfa4c4b8376b4bbf=sOdPqaAH; comment_author_email_311f7ebdbf2fdff1bfa4c4b8376b4bbf=testing%40example.com;
comment_author_url_311f7ebdbf2fdff1bfa4c4b8376b4bbf=http%3A%2F%2Fwww.example.com; wordpress_test_cookie=WP+Cookie+check;
ec_cart_id=KRZULVEOJJCQRXPJOVCUNFMMHEFDBE; PHPSESSID=aqceka9dkvqmo63rrm46ru828b
Content-Type: application/x-www-form-urlencoded
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Content-Length: 41
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: 192.168.1.5
Connection: Keep-alive

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

Recommendation

Upgrade to the latest version.

Outdated JavaScript libraries

You are using an outdated version of one or more JavaScript libraries. A more recent version is available. Although your version was not found to be affected by any security vulnerabilities, it is recommended to keep libraries up to date.

CWE
CWE-937

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

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

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

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

CVSS4
CVSS:4.0/AV:N/AC:H/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	High
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

Consult References for more information.

http://192.168.1.5/ Confidence: 95%

- jQuery UI Tooltip 1.10.3
  - URL: http://192.168.1.5/wordpress/
  - Detection method: The library's name and version were determined based on its dynamic behavior.
  - References:
    - https://jqueryui.com/download/

Request

```
GET /wordpress/ HTTP/1.1
Referer: http://192.168.1.5/
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: 192.168.1.5
Connection: Keep-alive
```

http://192.168.1.5/ Confidence: 95%

- Underscore.js 1.8.3
  - URL: http://192.168.1.5/wordpress/
  - Detection method: The library's name and version were determined based on its dynamic behavior.
  - References:
    - https://github.com/jashkenas/underscore/tags

Request

```
GET /wordpress/ HTTP/1.1
Referer: http://192.168.1.5/
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: 192.168.1.5
Connection: Keep-alive
```

Recommendation

Upgrade to the latest version.

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

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

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

Availability Impact	None

Integrity Impact	Low
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

Possible information disclosure.

http://192.168.1.5/ Verified

Request

```
GET / HTTP/1.1
Referer: http://192.168.1.5/
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: 192.168.1.5
Connection: Keep-alive
```

Recommendation

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

WordPress username enumeration

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

CWE
CWE-200

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

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

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

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

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

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

Impact

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

http://192.168.1.5/wordpress/

List of WordPress users for {'_nativeUrl': {'password': '', 'username': '', 'search': '', 'protocol': 'http', 'port': '', 'path': '/wordpress/', 'origin': 'http://192.168.1.5', 'href': 'http://192.168.1.5/wordpress/', 'hostname': '192.168.1.5', 'host': '192.168.1.5', 'hash': ''}}:

['admin']

Request

```
POST /wordpress//wp-login.php HTTP/1.1
Content-type: application/x-www-form-urlencoded
Cookie: comment_author_311f7ebdbf2fdff1bfa4c4b8376b4bbf=sOdPqaAH; comment_author_email_311f7ebdbf2fdff1bfa4c4b8376b4bbf=testing%40example.com;
comment_author_url_311f7ebdbf2fdff1bfa4c4b8376b4bbf=http%3A%2F%2Fwww.example.com; ec_cart_id=KRZULVEOJJCQRXPJOVCUNFMMHEFDBE;
PHPSESSID=aqceka9dkvqmo63rrm46ru828b
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: 192.168.1.5
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
Availability Impact to the Subsequent System	None

Impact

No impact is associated with this vulnerability.

http://192.168.1.5/wordpress/wp-login.php

Request

```
POST /wordpress//wp-login.php HTTP/1.1
Content-type: application/x-www-form-urlencoded
Cookie: ec_cart_id=GBBQYPNKBUSYMSPGDLURKTQEGRKPQF; PHPSESSID=nt36t21i6j2s3qvn17255ejgni
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: 192.168.1.5
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

WP Support Plus Responsive Ticket System Security Bypass

WordPress Plugin WP Support Plus Responsive Ticket System is prone to a security bypass vulnerability. Exploiting this issue may allow attackers to perform otherwise restricted actions and subsequently login as any user without knowing the password. WordPress Plugin WP Support Plus Responsive Ticket System version 7.1.4 is vulnerable; prior versions may also be affected.

CWE
CWE-287

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

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

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

Base Score	7.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity Impact	Low
Availability Impact	Low

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

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

Impact

http://192.168.1.5/wordpress/wp-content/plugins/wp-support-plus-responsive-ticket-system/

wp-support-plus-responsive-ticket-system v7.1.3-7.1.3

Recommendation

Update to plugin version 8.0.0 or latest

References

https://security.szurek.pl/wp-support-plus-responsive-ticket-system-713-privilege-escalation.html
https://security.szurek.pl/wp-support-plus-responsive-ticket-system-713-privilege-escalation.html

https://plugins.svn.wordpress.org/wp-support-plus-responsive-ticket-system/trunk/readme.txt
https://plugins.svn.wordpress.org/wp-support-plus-responsive-ticket-system/trunk/readme.txt

WordPress XML-RPC authentication brute force

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

CWE
CWE-521

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

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

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

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

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

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

Impact

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

http://192.168.1.5/wordpress/xmlrpc.php

Pattern found:

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

Request

```
POST /wordpress//xmlrpc.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Cookie: ec_cart_id=GBBQYPNKBUSYMSPGDLURKTQEGRKPQF; PHPSESSID=nt36t21i6j2s3qvn17255ejgni
Content-Length: 264
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0 Safari/537.36
Host: 192.168.1.5
Connection: Keep-alive

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

Recommendation

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

References

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

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

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

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

WordPress is a free and open-source content management system written in PHP and paired with a MariaDB database. On a multisite, users with Super Admin role can bypass explicit/additional hardening under certain conditions through object injection. This has been patched in WordPress version 5.8.3. Older affected versions are also fixed via security release, that go back till 3.7.37. We strongly recommend that you keep auto-updates enabled. There are no known workarounds for this issue.

CWE
CWE-502

CVSS3
CVSS:3.1/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://192.168.1.5/wordpress/

wordpress v5.2.23-5.2.23

References

CVE-2022-21663
https://nvd.nist.gov/vuln/detail/CVE-2022-21663

CKEditor Inclusion of Functionality from Untrusted Control Sphere Vulnerability

It was possible to execute a ReDoS-type attack inside CKEditor 4 before 4.16 by persuading a victim to paste crafted text into the Styles input of specific dialogs (in the Advanced Tab for Dialogs plugin).

CWE
CWE-829

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

Base Score	6.5
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:H/SC:N/SI:N/SA:N

Base Score	6.9
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None

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

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

Impact

http://192.168.1.5/

ckeditor v4.5.4-4.5.4

http://192.168.1.5/

ckeditor v4.5.4-4.5.4

References

CVE-2021-26271
https://nvd.nist.gov/vuln/detail/CVE-2021-26271

WP Support Plus Responsive Ticket System PHP Object Injection

WordPress Plugin WP Support Plus Responsive Ticket System 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 Plugin WP Support Plus Responsive Ticket System version 9.0.3 is vulnerable; prior versions may also be affected.

CWE
CWE-915

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

Access Vector	Network
Access Complexity	Low
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:C/C:L/I:L/A:L

Base Score	8.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Changed
Confidentiality	Low
Integrity Impact	Low
Availability Impact	Low

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

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

Impact

http://192.168.1.5/wordpress/wp-content/plugins/wp-support-plus-responsive-ticket-system/

wp-support-plus-responsive-ticket-system v7.1.3-7.1.3

Recommendation

Update to plugin version 9.0.4 or latest

References

https://www.pluginvulnerabilities.com/2018/02/16/our-proactive-monitoring-caught-a-php-object-injection-vulnerability-in-a-fairly-popular-plugin/
https://www.pluginvulnerabilities.com/2018/02/16/our-proactive-monitoring-caught-a-php-object-injection-vulnerability-in-a-fairly-popular-plugin/

A09 Security Logging and Monitoring Failures

Insufficient logging and monitoring, coupled with missing or ineffective integration with incident response, allows attackers to further attack systesm, maintain persistence, pivot to more systems, and tamper, extract, or destroy data. Most breach studies show time to detect a breach is over 200 days, typically detected by external parties rather than internal processes or monitoring.

No alerts in this category

A10 Server-Side Request Forgery

SSRF flaws occur whenever a web application is fetching a remote resource without validating the user-supplied URL. It allows an attacker to coerce the application to send a crafted request to an unexpected destination, even when protected by a firewall, VPN, or another type of network access control list (ACL).

WordPress Server-Side Request Forgery

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://192.168.1.5/wordpress/
wordpress v5.2.23-5.2.23

Recommendation

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

References

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

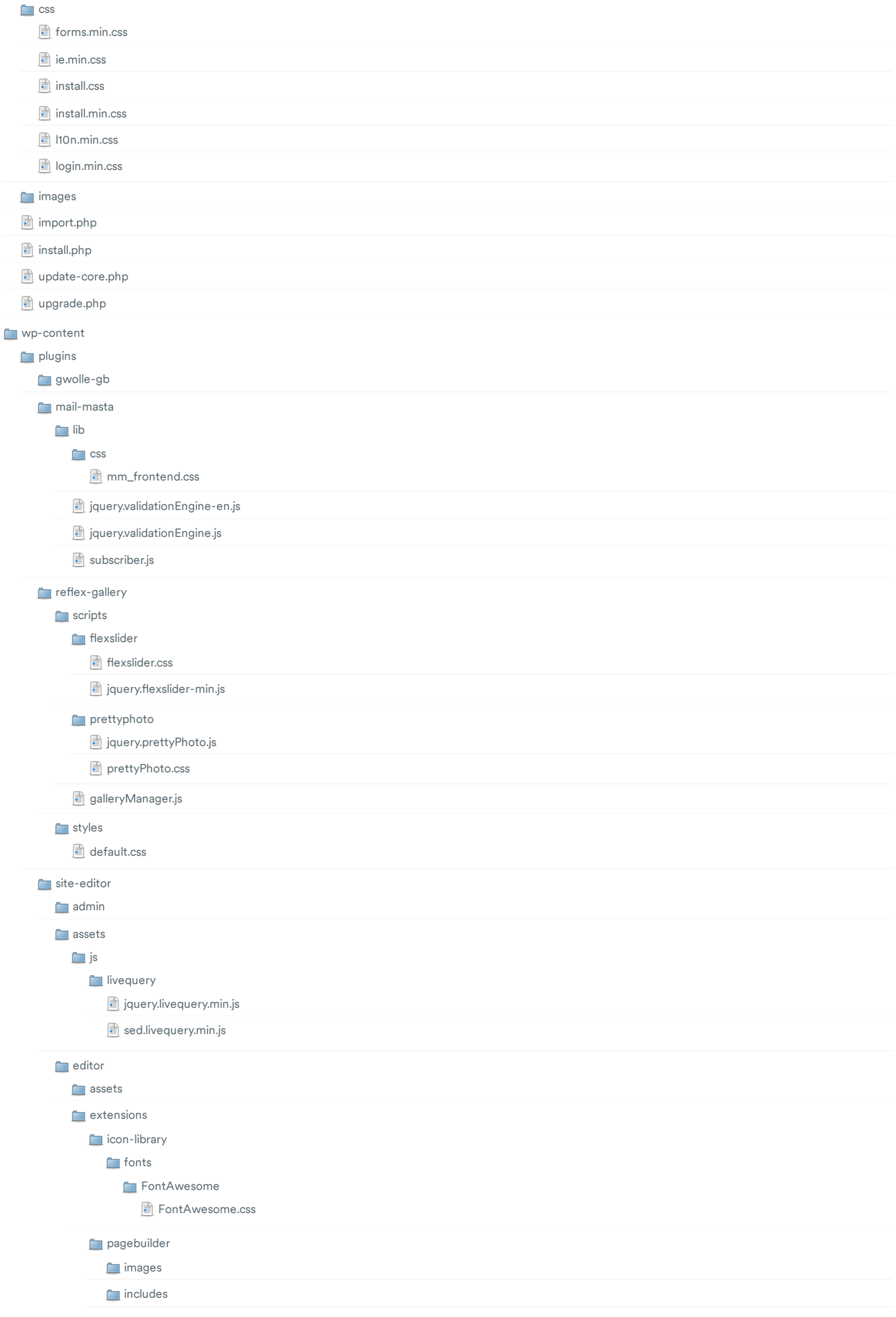
https://blog.sonarsource.com/wordpress-core-unauthenticated-blind-ssrf/
https://sploitus.com/exploit?id=WPEX-ID:C8814E6E-78B3-4F63-A1D3-6906A84C1F11
https://sploitus.com/exploit?id=WPEX-ID:C8814E6E-78B3-4F63-A1D3-6906A84C1F11

Coverage

- http://192.168.1.5
  - icons
  - wordpress
    - #fragments
      - content
    - index.php
      - 2019
        - 09
          - 09
            - hello-world
              - #fragments
                - comment-1
                - comment-10
                - comment-11
                - comment-12
                - comment-13
                - comment-14
                - comment-15
                - comment-16
                - comment-17
                - comment-18
                - comment-19
                - comment-2
                - comment-21
                - comment-22
                - comment-23
                - comment-24
                - comment-25
                - comment-27
                - comment-28
                - comment-29
                - comment-3
                - comment-30
                - comment-31
                - comment-32
                - comment-33
                - comment-34
                - comment-35
                - comment-36
                - comment-37
                - comment-38
                - comment-39
                - comment-4
                - comment-5
                - comment-6
                - comment-7
                - comment-8

- comment-9
- comments
- content
- respond
- embed
- feed

- author
  - admin
    - #fragments
      - content
    - feed
- category
  - uncategorized
    - #fragments
      - content
    - feed
- comments
  - feed
- feed
- open-ticket
- sample-page
- search
  - 1
    - feed
      - rss2
    - feed
      - rss2
    - the
      - feed
        - rss2
- wp-json
  - oembed
    - 1.0
      - embed
    - 1.0
  - wp
    - v2
      - categories
      - comments
      - media
      - posts
      - search
      - statuses
      - tags
      - taxonomies
      - types
      - users
    - v2
- wp-admin


css
forms.min.css
ie.min.css
install.css
install.min.css
l10n.min.css
login.min.css
images
import.php
install.php
update-core.php
upgrade.php
wp-content
plugins
gwolle-gb
mail-masta
lib
css
mm_frontend.css
jquery.validationEngine-en.js
jquery.validationEngine.js
subscriber.js
reflex-gallery
scripts
flexslider
flexslider.css
jquery.flexslider-min.js
prettyphoto
jquery.prettyPhoto.js
prettyPhoto.css
galleryManager.js
styles
default.css
site-editor
admin
assets
js
livequery
jquery.livequery.min.js
sed.livequery.min.js
editor
assets
extensions
icon-library
fonts
FontAwesome
FontAwesome.css
pagebuilder
images
includes

- modules
  - icons
  - image
  - menu
  - row
    - js
      - row.js
  - search
- view
- includes
- templates

framework
- assets
  - css
    - animate
      - animate.min.css
    - general.min.css
  - js
    - animate
      - wow.min.js
    - parallax
      - jquery.parallax.min.js
    - render.min.js
    - sed_app_site.min.js
- includes
- languages
- .gitignore
- package.json
- README.md
- readme.txt

slideshow-gallery
- css
  - colorbox.css
- js
  - colorbox.js
  - gallery.js

wp-easycart-data
- design
  - theme
    - base-responsive-v3
      - ec-store.css
      - ec-store.js

wp-easycart

wp-support-plus-responsive-ticket-system
- asset
  - css
    - display_ticket.css
    - jquery-ui.min.css
    - jquery-ui.structure.min.css

- jquery-ui.theme.min.css
- public.css
- images
- js
  - bootstrap
    - css
      - bootstrap.css
    - js
      - bootstrap.min.js
  - public_create_ticket.js
  - public.js
- lib
  - ckeditor
    - adapters
      - jquery.js
    - ckeditor.js

- wp-symposium
  - ajax
    - symposium_ajax_functions.php
    - symposium_bar_functions.php
    - symposium_forum_functions.php
    - symposium_group_functions.php
    - symposium_groups_functions.php
    - symposium_mail_functions.php
    - symposium_profile_functions.php
  - css
    - chat.css
    - jquery-ui-1.10.3.custom.css
    - jquery.fileupload-ui.css
    - wps.min.css
  - images
  - js
    - canvas-to-blob.min.js
    - jquery-ui-1.10.3.custom.min.js
    - jquery.fileupload-fp.js
    - jquery.fileupload-ui.js
    - jquery.fileupload.js
    - jquery.iframe-transport.js
    - jscharts.min.js
    - jwplayer.js
    - load-image.min.js
    - tmpl.min.js
    - wps.min.js
  - tiny_mce
    - themes
      - advanced
        - skins
          - wps.css
  - uploadify

- get_profile_avatar.php
- wp-symposium
  - uploadify
    - uploadify.php
  - get_album_item.php
  - readme.txt
- themes
  - twentysixteen
    - css
      - blocks.css
      - ie.css
      - ie7.css
      - ie8.css
    - genericons
      - genericons.css
    - js
      - functions.js
      - html5.js
      - skip-link-focus-fix.js
    - style.css
- upgrade
- uploads
- wp-includes
  - blocks
  - certificates
  - css
    - dist
      - block-library
        - style.min.css
        - theme.min.css
    - buttons.min.css
    - dashicons.min.css
    - jquery-ui-dialog.min.css
  - customize
  - fonts
  - ID3
    - getid3.lib.php
    - getid3.php
    - license.commercial.txt
    - license.txt
    - module.audio-video.asf.php
    - module.audio-video.flv.php
    - module.audio-video.matroska.php
    - module.audio-video.quicktime.php
    - module.audio-video.riff.php
    - module.audio.ac3.php
    - module.audio.dts.php
    - module.audio.flac.php
    - module.audio.mp3.php

- module.audio.ogg.php
- module.tag.apetag.php
- module.tag.id3v1.php
- module.tag.id3v2.php
- module.tag.lyrics3.php
- readme.txt
- images
- IXR
- js
  - jquery
    - ui
      - accordion.min.js
      - button.min.js
      - core.min.js
      - datepicker.min.js
      - dialog.min.js
      - draggable.min.js
      - mouse.min.js
      - position.min.js
      - resizable.min.js
      - widget.min.js
    - jquery-migrate.min.js
    - jquery.js
  - comment-reply.min.js
  - underscore.min.js
  - wp-embed.min.js
  - wp-emoji-release.min.js
- pomo
- random_compat
- Requests
- rest-api
- SimplePie
- sodium_compat
- Text
- theme-compat
- widgets
- admin-bar.php
- atomlib.php
- author-template.php
- blocks.php
- bookmark-template.php
- bookmark.php
- cache.php
- canonical.php
- capabilities.php
- category-template.php
- category.php
- class-feed.php
- class-http.php

class-IXR.php
class-json.php
class-oembed.php
class-phpass.php
class-phpmailer.php
class-pop3.php
class-requests.php
class-simplepie.php
class-smtp.php
class-snoopy.php
class-walker-category-dropdown.php
class-walker-category.php
class-walker-comment.php
class-walker-nav-menu.php
class-walker-page-dropdown.php
class-walker-page.php
class-wp-admin-bar.php
class-wp-ajax-response.php
class-wp-block-parser.php
class-wp-block-type-registry.php
class-wp-block-type.php
class-wp-comment-query.php
class-wp-comment.php
class-wp-customize-control.php
class-wp-customize-manager.php
class-wp-customize-nav-menus.php
class-wp-customize-panel.php
class-wp-customize-section.php
class-wp-customize-setting.php
class-wp-customize-widgets.php
class-wp-dependency.php
class-wp-editor.php
class-wp-embed.php
class-wp-error.php
class-wp-fatal-error-handler.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-paused-extensions-storage.php
class-wp-post-type.php
class-wp-post.php
class-wp-query.php
class-wp-recovery-mode-cookie-service.php
class-wp-recovery-mode-email-service.php
class-wp-recovery-mode-key-service.php
class-wp-recovery-mode-link-service.php
class-wp-recovery-mode.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
- error-protection.php
- feed-atom-comments.php
- feed-atom.php
- feed-rdf.php
- feed-rss.php
- feed-rss2-comments.php
- feed-rss2.php
- feed.php
- formatting.php
- functions.php
- functions.wp-scripts.php
- functions.wp-styles.php
- general-template.php
- http.php
- kses.php
- l10n.php
- link-template.php
- load.php
- locale.php
- media-template.php
- media.php
- meta.php
- ms-blogs.php
- ms-default-constants.php
- ms-default-filters.php
- ms-deprecated.php
- ms-files.php
- ms-functions.php
- ms-load.php
- ms-network.php
- ms-settings.php
- wlwmanifest.xml
- license.txt
- readme.html
- wp-comments-post.php
- wp-login.php