Vulnerability Advisories

Wordfence is authorized by the Common Vulnerabilities and Exposures (CVE®) Program as a CNA, or CVE Numbering Authority. As a CNA, Wordfence assigns CVE IDs for new vulnerabilities in WordPress Core, WordPress Plugins and WordPress Themes.

Assigned CVE IDs and the vulnerability details are published below. For more information about submitting vulnerabilities to Wordfence for CVE ID assignment, please refer to our vulnerability disclosure policy.

This page is no longer maintained, please visit Wordfence Intelligence Community Edition for the latest Information on Vulnerabilities.

demon image annotation <= 4.7 – Cross-Site Request Forgery to Cross-Site Scripting

Affected Plugin: demon image annotation
Plugin Slug: demon-image-annotation
Affected Versions: <= 4.7
CVE ID: CVE-2022-2864
CVSS Score: 8.8 (High)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:N
Researcher/s: Yamato Kamioka
Fully Patched Version: 4.8
Recommended Remediation: Update to version 4.8, or newer.
Publication Date: 2022-09-21

The demon image annotation plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 4.7. This is due to missing nonce validation in the ~/includes/settings.php file. This makes it possible for unauthenticated attackers to modify the plugin's settings and inject malicious web scripts via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.

SearchWP Live Ajax Search <= 1.6.2 – Directory Traversal and Local File Inclusion

Affected Plugin: SearchWP Live Ajax Search
Plugin Slug: searchwp-live-ajax-search
Affected Versions: <= 1.6.2
CVE ID: CVE-2022-3227
CVSS Score: 8.2 (High)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:N
Researcher/s: Muhammad Zeeshan (Xib3rR4dAr)
Fully Patched Version: 1.6.3
Recommended Remediation: Update to version 1.6.3, or newer.
Publication Date: 2022-09-15

The SearchWP Live Ajax Search plugin for WordPress is vulnerable to Directory Traversal via the `swpengine` parameter used by the `searchwp_live_search` AJAX action in versions up to, and including, 1.6.2. This allows unauthenticated attackers to include and execute arbitrary local PHP files.

Wordfence Security – Firewall & Malware Scan <= 7.6.0 – Authenticated (Admin+) Stored Cross-Site Scripting

Affected Plugin: Wordfence Security – Firewall & Malware Scan
Plugin Slug: wordfence
Affected Versions: <= 7.6.0
CVE ID: CVE-2022-3144
CVSS Score: 4.4 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:C/C:L/I:L/A:N
Researcher/s: Ori Gabriel
Fully Patched Version: 7.6.1
Recommended Remediation: Update to version 7.6.1, or newer.
Publication Date: 2022-09-06

The Wordfence Security – Firewall & Malware Scan plugin for WordPress is vulnerable to Stored Cross-Site Scripting in versions up to, and including, 7.6.0 via a setting on the options page due to insufficient escaping on the stored value. This makes it possible for authenticated users, with administrative privileges, to inject malicious web scripts into the setting that executes whenever a user accesses a page displaying the affected setting on sites running a vulnerable version. This is unlikely to be exploited in the wild and would require an attacker gain access to an administrative user account or trick a site's administrator into injecting a script into the field themself (via self XSS).

WP Cerber Security <= 9.0 – User Enumeration Bypass

Affected Plugin: WP Cerber Security, Anti-spam & Malware Scan
Plugin Slug: wp-cerber
Affected Versions: <= 9.0
CVE ID: CVE-2022-2939
CVSS Score: 5.3 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
Researcher/s: Margaux DABERT (Intrinsec)
Fully Patched Version: 9.1
Recommended Remediation: Update to version 9.1, or newer.
Publication Date: 2022-09-02

The WP Cerber Security plugin for WordPress is vulnerable to security protection bypass in versions up to, and including 9.0, that makes user enumeration possible. This is due to improper validation on the value supplied through the 'author' parameter found in the ~/cerber-load.php file. In vulnerable versions, the plugin only blocks requests if the value supplied is numeric, making it possible for attackers to supply additional non-numeric characters to bypass the protection. The non-numeric characters are stripped and the user requested is displayed. This can be used by unauthenticated attackers to gather information about users that can targeted in further attacks.

Image Hover Effects Ultimate <= 9.7.3 – Authenticated Stored Cross-Site Scripting via Media URL

Affected Plugin: Image Hover Effects Ultimate (Image Gallery, Effects, Lightbox, Comparison or Magnifier)
Plugin Slug: image-hover-effects-ultimate
Affected Versions: <= 9.7.3
CVE ID: CVE-2022-2935
CVSS Score: 6.4 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:N
Researcher/s: Zhouyuan Yang
Fully Patched Version: 9.8.0
Recommended Remediation: Update to version 9.8.0, or newer.
Publication Date: 2022-08-31

The Image Hover Effects Ultimate plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Media Image URL value that can be added to an Image Hover in versions up to, and including, 9.7.3 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. By default, the plugin only allows administrators access to edit Image Hovers, however, if a site admin makes the plugin's features available to lower privileged users through the 'Who Can Edit?' setting then this can be exploited by those users.

Image Hover Effects Ultimate <= 9.7.3 – Authenticated Stored Cross-Site Scripting via Video Link

Affected Plugin: Image Hover Effects Ultimate (Image Gallery, Effects, Lightbox, Comparison or Magnifier)
Plugin Slug: image-hover-effects-ultimate
Affected Versions: <= 9.7.3
CVE ID: CVE-2022-2936

CVSS Score: 6.4 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:N

Publication Date: 2022-08-31

The Image Hover Effects Ultimate plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Video Link values that can be added to an Image Hover in versions up to, and including, 9.7.3 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. By default, the plugin only allows administrators access to edit Image Hovers, however, if a site admin makes the plugin's features available to lower privileged users through the 'Who Can Edit?' setting then this can be exploited by those users.

Image Hover Effects Ultimate <= 9.7.3 – Authenticated Stored Cross-Site Scripting via Title & Description

Affected Plugin: Image Hover Effects Ultimate (Image Gallery, Effects, Lightbox, Comparison or Magnifier)
Plugin Slug: image-hover-effects-ultimate
Affected Versions: <= 9.7.3
CVE ID: CVE-2022-2937
CVSS Score: 6.4 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:N
Researcher/s: Zhouyuan Yang
Fully Patched Version: 9.8.0
Recommended Remediation: Update to version 9.8.0, or newer.
Publication Date: 2022-08-31

The Image Hover Effects Ultimate plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Title & Description values that can be added to an Image Hover in versions up to, and including, 9.7.3 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. By default, the plugin only allows administrators access to edit Image Hovers, however, if a site admin makes the plugin's features available to lower privileged users through the 'Who Can Edit?' setting then this can be exploited by those users.

Beaver Builder – WordPress Page Builder <= 2.5.5.2 – Authenticated Stored Cross-Site Scripting via Caption – On Hover

Affected Plugin: Beaver Builder – WordPress Page Builder
Plugin Slug: beaver-builder-lite-version
Affected Versions: <= 2.5.5.2
CVE ID: CVE-2022-2517
CVSS Score: 6.4 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:N
Researcher/s: Zhouyuan Yang
Fully Patched Version: 2.5.5.3
Recommended Remediation: Update to version 2.5.5.2, or newer.
Publication Date: 2022-08-30

The Beaver Builder – WordPress Page Builder for WordPress is vulnerable to Stored Cross-Site Scripting via the 'Caption – On Hover' value associated with images in versions up to, and including, 2.5.5.2 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers with access to the Beaver Builder editor to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.

Beaver Builder – WordPress Page Builder <= 2.5.5.2 – Authenticated Stored Cross-Site Scripting via 'caption'

Affected Plugin: Beaver Builder – WordPress Page Builder
Plugin Slug: beaver-builder-lite-version
Affected Versions: <= 2.5.5.2
CVE ID: CVE-2022-2695
CVSS Score: 6.4 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:N
Researcher/s: Zhouyuan Yang
Fully Patched Version: 2.5.5.3
Recommended Remediation: Update to version 2.5.5.2, or newer.
Publication Date: 2022-08-30

The Beaver Builder – WordPress Page Builder for WordPress is vulnerable to Stored Cross-Site Scripting via the 'caption' parameter added to images via the media uploader in versions up to, and including, 2.5.5.2 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers with access to the Beaver Builder editor and the ability to upload media files to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.

Beaver Builder – WordPress Page Builder <= 2.5.5.2 – Authenticated Stored Cross-Site Scripting via Text Editor

Affected Plugin: Beaver Builder – WordPress Page Builder
Plugin Slug: beaver-builder-lite-version
Affected Versions: <= 2.5.5.2
CVE ID: CVE-2022-2716
CVSS Score: 6.4 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:N
Researcher/s: Zhouyuan Yang
Fully Patched Version: 2.5.5.3
Recommended Remediation: Update to version 2.5.5.2, or newer.
Publication Date: 2022-08-29

The Beaver Builder – WordPress Page Builder for WordPress is vulnerable to Stored Cross-Site Scripting via the 'Text Editor' block in versions up to, and including, 2.5.5.2 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers with access to the Beaver Builder editor to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.

Beaver Builder – WordPress Page Builder <= 2.5.5.2 – Authenticated Stored Cross-Site Scripting via Image URL

Affected Plugin: Beaver Builder – WordPress Page Builder
Plugin Slug: beaver-builder-lite-version
Affected Versions: <= 2.5.5.2
CVE ID: CVE-2022-2934
CVSS Score: 6.4 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:N
Researcher/s: Zhouyuan Yang
Fully Patched Version: 2.5.5.3
Recommended Remediation: Update to version 2.5.5.2, or newer.
Publication Date: 2022-08-29

The Beaver Builder – WordPress Page Builder for WordPress is vulnerable to Stored Cross-Site Scripting via the 'Image URL' value found in the Media block in versions up to, and including, 2.5.5.2 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers with access to the Beaver Builder editor to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.

Visual Composer Website Builder <= 45.0 – Authenticated Stored Cross-Site Scripting via 'Title'

Affected Plugin: Visual Composer Website Builder, Landing Page Builder, Custom Theme Builder, Maintenance Mode & Coming Soon Pages
Plugin Slug: visualcomposer
Affected Versions: <= 45.0
CVE ID: CVE-2022-2516
CVSS Score: 6.4 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:N
Researcher/s: Zhouyuan Yang
Fully Patched Version: 45.0.1
Recommended Remediation: Update to version 45.0.1, or newer.
Publication Date: 2022-08-29

The Visual Composer Website Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the post/page 'Title' value in versions up to, and including, 45.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers with access to the visual composer editor to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.

Visual Composer Website Builder <= 45.0 – Authenticated Stored Cross-

Affected Plugin: Visual Composer Website Builder, Landing Page Builder, Custom Theme Builder, Maintenance Mode & Coming Soon Pages
Plugin Slug: visualcomposer
Affected Versions: <= 45.0
CVE ID: CVE-2022-2430
CVSS Score: 6.4 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:N
Researcher/s: Zhouyuan Yang
Fully Patched Version: 45.0.1
Recommended Remediation: Update to version 45.0.1, or newer.
Publication Date: 2022-08-29

The Visual Composer Website Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'Text Block' feature in versions up to, and including, 45.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers with access to the visual composer editor to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.

Ultimate SMS Notifications for WooCommerce <= 1.4.1 – CSV Injection

Affected Plugin: Ultimate SMS Notifications for WooCommerce
Plugin Slug: ultimate-sms-notifications
Affected Versions: <= 1.4.1
CVE ID: CVE-2022-2429
CVSS Score: 6.5 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:L
Researcher/s: Zhouyuan Yang
Fully Patched Version: 1.4.2
Recommended Remediation: Update to version 1.4.2, or newer.
Publication Date: 2022-08-29

The Ultimate SMS Notifications for WooCommerce plugin for WordPress is vulnerable to CSV Injection in versions up to, and including, 1.4.1 via the 'Export Utility' functionality. This makes it possible for authenticated attackers, such as a subscriber, to add untrusted input into billing information like their First Name that will embed into the exported CSV file triggered by an administrator and can result in code execution when these files are downloaded and opened on a local system with a vulnerable configuration.

WP Users Exporter <= 1.4.2 – CSV Injection

Affected Plugin: WP Users Exporter
Plugin Slug: wp-users-exporter
Affected Versions: <= 1.4.2
CVE ID: CVE-2022-3026
CVSS Score: 6.5 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:L
Researcher/s: Zhouyuan Yang
Fully Patched Version: No patch available, plugin closed for download.
Recommended Remediation: Uninstall Plugin.
Publication Date: 2022-08-29

The WP Users Exporter plugin for WordPress is vulnerable to CSV Injection in versions up to, and including, 1.4.2 via the 'Export Users' functionality. This makes it possible for authenticated attackers, such as a subscriber, to add untrusted input into profile information like First Names that will embed into the exported CSV file triggered by an administrator and can result in code execution when these files are downloaded and opened on a local system with a vulnerable configuration.

WordPress Infinite Scroll – Ajax Load More <= 5.5.3 – Arbitrary File Read

Affected Plugin: WordPress Infinite Scroll – Ajax Load More
Plugin Slug: ajax-load-more
Affected Versions: <= 5.5.3
CVE ID: CVE-2022-2943
CVSS Score: 4.9 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N
Researcher/s: Muhammad Zeeshan (Xib3rR4dAr)
Fully Patched Version: 5.5.4
Recommended Remediation: Update to version 5.5.4, or newer.
Publication Date: 2022-08-22

The WordPress Infinite Scroll – Ajax Load More plugin for WordPress is vulnerable to arbitrary file reading in versions up to, and including, 5.5.3 due to insufficient file path validation on the alm_repeaters_export() function. This makes it possible for authenticated attackers, with administrative privileges, to download arbitrary files hosted on the server that may contain sensitive content, such as the wp-config.php file.

WordPress Infinite Scroll – Ajax Load More <= 5.5.3 – Directory Traversal

Affected Plugin: WordPress Infinite Scroll – Ajax Load More
Plugin Slug: ajax-load-more
Affected Versions: <= 5.5.3
CVE ID: CVE-2022-2945
CVSS Score: 4.9 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N
Researcher/s: Muhammad Zeeshan (Xib3rR4dAr)
Fully Patched Version: 5.5.4
Recommended Remediation: Update to version 5.5.4, or newer.
Publication Date: 2022-08-22

The WordPress Infinite Scroll – Ajax Load More plugin for WordPress is vulnerable to Directory Traversal in versions up to, and including, 5.5.3 via the 'type' parameter found in the alm_get_layout() function. This makes it possible for authenticated attackers, with administrative permissions, to read the contents of arbitrary files on the server, which can contain sensitive information.

WordPress Infinite Scroll – Ajax Load More <= 5.5.3 – Cross-Site Request Forgery to PHAR Deserialization

Affected Plugin: WordPress Infinite Scroll – Ajax Load More
Plugin Slug: ajax-load-more
Affected Versions: <= 5.5.3
CVE ID: CVE-2022-2433
CVSS Score: 8.8 (High)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
Researcher/s: Rasoul Jahanshahi
Fully Patched Version: 5.5.4
Recommended Remediation: Update to version 5.5.4, or newer.
Publication Date: 2022-08-22

The WordPress Infinite Scroll – Ajax Load More plugin for WordPress is vulnerable to deserialization of untrusted input via the 'alm_repeaters_export' parameter in versions up to, and including 5.5.3. This makes it possible for unauthenticated users to call files using a PHAR wrapper, granted they can trick a site administrator into performing an action such as clicking on a link, that will deserialize and call arbitrary PHP Objects that can be used to perform a variety of malicious actions granted a POP chain is also present. It also requires that the attacker is successful in uploading a file with the serialized payload.

WP-UserOnline <= 2.88.0 – Authenticated (Admin+) Stored Cross-Site Scripting

Affected Plugin: WP-UserOnline
Plugin Slug: wp-useronline
Affected Versions: <= 2.88.0
CVE ID: CVE-2022-2941
CVSS Score: 5.5 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:L/I:L/A:N
Researcher/s: Juampa Rodríguez
Fully Patched Version: 2.88.1
Recommended Remediation: Update to version 2.88.1, or newer.
Publication Date: 2022-08-22

The WP-UserOnline plugin for WordPress has multiple Stored Cross-Site Scripting vulnerabilities in versions up to, and including 2.88.0. This is due to the fact that all fields in the "Naming Conventions" section do not properly sanitize user input, nor escape it on output. This makes it possible for authenticated attackers, with administrative privileges, to inject JavaScript code into the setting that will execute whenever a user accesses the injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.

Migration, Backup, Staging – WPvivid <= 0.9.74 – Authenticated

Affected Plugin: Migration, Backup, Staging – WPvivid
Plugin Slug: wpvivid-backuprestore
Affected Versions: <= 0.9.74
CVE ID: CVE-2022-2442
CVSS Score: 7.2 (High)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H
Researcher/s: Rasoul Jahanshahi
Fully Patched Version: 0.9.75
Recommended Remediation: Update to version 0.9.75, or newer.
Publication Date: 2022-08-17

The Migration, Backup, Staging – WPvivid plugin for WordPress is vulnerable to deserialization of untrusted input via the 'path' parameter in versions up to, and including 0.9.74. This makes it possible for authenticated attackers with administrative privileges to call files using a PHAR wrapper that will deserialize and call arbitrary PHP Objects that can be used to perform a variety of malicious actions granted a POP chain is also present. It also requires that the attacker is successful in uploading a file with the serialized payload.

Download Manager <= 3.2.49 – Authenticated (Contributor+) PHAR Deserialization

Affected Plugin: Download Manager
Plugin Slug: download-manager
Affected Versions: <= 3.2.49
CVE ID: CVE-2022-2436
CVSS Score: 8.8 (High)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
Researcher/s: Rasoul Jahanshahi
Fully Patched Version: 3.2.50
Recommended Remediation: Update to version 3.2.50, or newer.
Publication Date: 2022-08-17

The Download Manager plugin for WordPress is vulnerable to deserialization of untrusted input via the 'file[package_dir]' parameter in versions up to, and including 3.2.49. This makes it possible for authenticated attackers with contributor privileges and above to call files using a PHAR wrapper that will deserialize the data and call arbitrary PHP Objects that can be used to perform a variety of malicious actions granted a POP chain is also present. It also requires that the attacker is successful in uploading a file with the serialized payload.

All-in-One Video Gallery 2.5.8 – 2.6.0 – Arbitrary File Download & Server-Side Request Forgery

Affected Plugin: All-in-One Video Gallery
Plugin Slug: all-in-one-video-gallery
Affected Versions: 2.5.8 – 2.6.0
CVE ID: CVE-2022-2633
CVSS Score: 7.5 (High)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
Researcher/s: Gabriele Zuddas
Fully Patched Version: 2.6.1
Recommended Remediation: Update to version 2.6.1, or newer.
Publication Date: 2022-08-17

The All-in-One Video Gallery plugin for WordPress is vulnerable to arbitrary file downloads and blind server-side request forgery via the 'dl' parameter found in the ~/public/video.php file in versions up to, and including 2.6.0. This makes it possible for unauthenticated users to download sensitive files hosted on the affected server and forge requests to the server.

Broken Link Checker <= 1.11.16 – Authenticated (Admin+) PHAR Deserialization

Affected Plugin: Broken Link Checker
Plugin Slug: broken-link-checker
Affected Versions: <= 1.11.16
CVE ID: CVE-2022-2438
CVSS Score: 7.2 (High)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H
Researcher/s: Rasoul Jahanshahi
Fully Patched Version: 1.11.17
Recommended Remediation: Update to version 1.11.17, or newer.
Publication Date: 2022-08-16

The Broken Link Checker plugin for WordPress is vulnerable to deserialization of untrusted input via the 'Slog_file' value in versions up to, and including 1.11.16. This makes it possible for authenticated attackers with administrative privileges and above to call files using a PHAR wrapper that will deserialize the data and call arbitrary PHP Objects that can be used to perform a variety of malicious actions granted a POP chain is also present. It also requires that the attacker is successful in uploading a file with the serialized payload.

JoomSport – for Sports: Team & League, Football, Hockey & more <= 5.2.5 – Authenticated (Admin+) SQL Injection via orderby

Affected Plugin: JoomSport – for Sports: Team & League, Football, Hockey & more
Plugin Slug: joomsport-sports-league-results-management
Affected Versions: <= 5.2.5
CVE ID: CVE-2022-2717
CVSS Score: 7.2 (High)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H
Researcher/s: salim al-wahaibi
Fully Patched Version: 5.2.6
Recommended Remediation: Update to version 5.2.6, or newer.
Publication Date: 2022-08-08

The JoomSport – for Sports: Team & League, Football, Hockey & more plugin for WordPress is vulnerable to SQL Injection via the 'orderby' parameter on the joomsport-events-form page in versions up to, and including, 5.2.5 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with administrative privileges, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.

JoomSport – for Sports: Team & League, Football, Hockey & more <= 5.2.5 – Authenticated (Admin+) SQL Injection via orderby

Affected Plugin: JoomSport – for Sports: Team & League, Football, Hockey & more
Plugin Slug: joomsport-sports-league-results-management
Affected Versions: <= 5.2.5
CVE ID: CVE-2022-2718
CVSS Score: 7.2 (High)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H
Researcher/s: salim al-wahaibi
Fully Patched Version: 5.2.6
Recommended Remediation: Update to version 5.2.6, or newer.
Publication Date: 2022-08-08

The JoomSport – for Sports: Team & League, Football, Hockey & more plugin for WordPress is vulnerable to SQL Injection via the 'orderby' parameter on the joomsport-page-extrafields page in versions up to, and including, 5.2.5 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with administrative privileges, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.

String Locator <= 2.5.0 – Authenticated PHAR Deserialization

Affected Plugin: String Locator
Plugin Slug: string-locator
Affected Versions: <= 2.5.0
CVE ID: CVE-2022-2434
CVSS Score: 8.8 (High)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
Researcher/s: Rasoul Jahanshahi
Fully Patched Version: 2.6.0

Recommended Remediation: Update to version 2.6.0, or newer.
Publication Date: 2022-08-08

trick a site administrator into performing an action such as clicking on a link (CSRF), that will deserialize and call arbitrary PHP Objects that can be used to perform a variety of malicious actions granted a POP chain is also present. It also requires that the attacker is successful in uploading a file with the serialized payload.

uContext for Clickbank <= 3.9.1 – Cross-Site Request Forgery to Cross-Site Scripting

Affected Plugin: uContext for Clickbank
Plugin Slug: ucontext
Affected Versions: <= 3.9.1
CVE ID: CVE-2022-2542
CVSS Score: 8.8 (High)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
Researcher/s: Hayato Takizawa
Fully Patched Version: No patch available, plugin closed for download.
Recommended Remediation: Uninstall Plugin.
Publication Date: 2022-08-02

The uContext for Clickbank plugin for WordPress is vulnerable to Cross-Site Request Forgery to Cross-Site Scripting in versions up to, and including 3.9.1. This is due to missing nonce validation in the ~/app/sites/ajax/actions/keyword_save.php file that is called via the doAjax() function. This makes it possible for unauthenticated attackers to modify the plugin's settings and inject malicious web scripts via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.

uContext for Amazon <= 3.9.1 – Cross-Site Request Forgery to Cross-Site Scripting

Affected Plugin: uContext for Amazon
Plugin Slug: ucontext-for-amazon
Affected Versions: <= 3.9.1
CVE ID: CVE-2022-2541
CVSS Score: 8.8 (High)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
Researcher/s: Hayato Takizawa
Fully Patched Version: No patch available, plugin closed for download.
Recommended Remediation: Uninstall Plugin.
Publication Date: 2022-08-02

The uContext for Amazon plugin for WordPress is vulnerable to Cross-Site Request Forgery to Cross-Site Scripting in versions up to, and including 3.9.1. This is due to missing nonce validation in the ~/app/sites/ajax/actions/keyword_save.php file that is called via the doAjax() function. This makes it possible for unauthenticated attackers to modify the plugin's settings and inject malicious web scripts via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.

Link Optimizer Lite <= 1.4.5 – Cross-Site Request Forgery to Cross-Site Scripting

Affected Plugin: Link Optimizer Lite
Plugin Slug: link-optimizer-lite
Affected Versions: <= 1.4.5
CVE ID: CVE-2022-2540
CVSS Score: 8.8 (High)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
Researcher/s: Hayato Takizawa
Fully Patched Version: No patch available, plugin closed for download.
Recommended Remediation: Uninstall Plugin.
Publication Date: 2022-08-02

The Link Optimizer Lite plugin for WordPress is vulnerable to Cross-Site Request Forgery to Cross-Site Scripting in versions up to, and including 1.4.5. This is due to missing nonce validation on the admin_page function found in the ~/admin.php file. This makes it possible for unauthenticated attackers to modify the plugin's settings and inject malicious web scripts via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.

Banner Cycler <= 1.4 – Cross-Site Request Forgery to Cross-Site Scripting

Affected Plugin: Banner Cycler
Plugin Slug: banner-cycler
Affected Versions: <= 1.4
CVE ID: CVE-2022-2233
CVSS Score: 8.8 (High)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
Researcher/s: MOTEKI TAKERU
Fully Patched Version: No patch available, plugin closed for download.
Recommended Remediation: Uninstall Plugin.
Publication Date: 2022-08-02

The Banner Cycler plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including 1.4. This is due to missing nonce protection on the pabc_admin_slides_postback() function found in the ~/admin/admin.php file. This makes it possible for unauthenticated attackers to inject malicious web scripts into the page, granted they can trick a site's administrator into performing an action such as clicking on a link

Simple SEO <= 1.7.91 – Contributor+ Stored Cross-Site Scripting

Affected Plugin: Simple SEO
Plugin Slug: cds-simple-seo
Affected Versions: <= 1.7.91
CVE ID: CVE-2022-1628
CVSS Score: 6.4 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:N
Researcher/s: Jörgson
Fully Patched Version: 1.7.92
Recommended Remediation: Update to version 1.7.92, or newer.
Publication Date: 2022-07-29

The Simple SEO plugin for WordPress is vulnerable to attribute-based stored Cross-Site Scripting in versions up to, and including 1.7.91, due to insufficient sanitization or escaping on the SEO social and standard title parameters. This can be exploited by authenticated users with Contributor and above permissions to inject arbitrary web scripts into posts/pages that execute whenever an administrator access the page.

Transposh WordPress Translation <= 1.0.8.1 – Sensitive Information Disclosure

Affected Plugin: Transposh WordPress Translation
Plugin Slug: transposh-translation-filter-for-wordpress
Affected Versions: <= 1.0.8.1
CVE ID: CVE-2022-2462
CVSS Score: 5.3 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
Researcher/s: Julien Ahrens
Fully Patched Version: No patch available, plugin closed for download.
Recommended Remediation: Uninstall Plugin.
Publication Date: 2022-07-25

The Transposh WordPress Translation plugin for WordPress is vulnerable to sensitive information disclosure to unauthenticated users in versions up to, and including, 1.0.8.1. This is due to insufficient permissions checking on the 'tp_history' AJAX action and insufficient restriction on the data returned in the response. This makes it possible for unauthenticated users to exfiltrate usernames of individuals who have translated text.

Transposh WordPress Translation <= 1.0.8.1 – Unauthorized Settings Change

Affected Plugin: Transposh WordPress Translation
Plugin Slug: transposh-translation-filter-for-wordpress
Affected Versions: <= 1.0.8.1

CVE ID: CVE-2022-2461
CVSS Score: 5.3 (Medium)

Recommended Remediation: Uninstall Plugin.
Publication Date: 2022-07-25

The Transposh WordPress Translation plugin for WordPress is vulnerable to unauthorized setting changes by unauthenticated users in versions up to, and including, 1.0.8.1. This is due to insufficient permissions checking on the 'tp_translation' AJAX action and default settings which makes it possible for unauthenticated attackers to influence the data shown on the site.

Stockists Manager for Woocommerce <= 1.0.2.1 – Cross-Site Request Forgery to Stored Cross-Site Scripting

Affected Plugin: Stockists Manager for Woocommerce
Plugin Slug: stockists-manager
Affected Versions: <= 1.0.2.1
CVE ID: CVE-2022-2518
CVSS Score: 8.8 (High)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
Researcher/s: Yuta Kikuchi
Fully Patched Version: No patch available, plugin closed for download.
Recommended Remediation: Uninstall Plugin.
Publication Date: 2022-07-22

The Stockists Manager for Woocommerce plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.0.2.1. This is due to missing nonce validation on the stockist_settings_main() function. This makes it possible for unauthenticated attackers to modify the plugin's settings and inject malicious web scripts via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.

Simple Banner <= 2.11.0 – Authenticated Stored Cross-Site Scripting

Affected Plugin: Simple Banner
Plugin Slug: simple-banner
Affected Versions: <= 2.11.0
CVE ID: CVE-2022-2515
CVSS Score: 6.4 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:N
Researcher/s: Muhammad Zeeshan (Xib3rR4dAr)
Fully Patched Version: 2.12.0
Recommended Remediation: Update to version 2.12.0, or newer.
Publication Date: 2022-07-22

The Simple Banner plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the `pro_version_activation_code` parameter in versions up to, and including, 2.11.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, including those without administrative capabilities when access is granted to those users, to inject arbitrary web scripts in page that will execute whenever a user role having access to "Simple Banner" accesses the plugin's settings.

WP-UserOnline <= 2.87.6 – Authenticated (Admin+) Stored Cross-Site Scripting

Affected Plugin: WP-UserOnline
Plugin Slug: wp-useronline
Affected Versions: <= 2.87.6
CVE ID: CVE-2022-2473
CVSS Score: 5.5 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:L/I:L/A:N
Researcher/s: steffin stanly
Fully Patched Version: 2.88.0
Recommended Remediation: Update to version 2.88.0, or newer.
Publication Date: 2022-07-19

The WP-UserOnline plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'templates[browsingpage]' parameter in versions up to, and including, 2.87.6 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers with administrative capabilities and above to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. The only affects multi-site installations and installations where unfiltered_html is disabled.

Feed Them Social – for Twitter feed, Youtube and more <= 2.9.8.5 – Unauthenticated PHAR Deserialization

Affected Plugin: Feed Them Social – for Twitter feed, Youtube and more
Plugin Slug: feed-them-social
Affected Versions: <= 2.9.8.5
CVE ID: CVE-2022-2437
CVSS Score: 8.8 (High)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Researcher/s: Rasoul Jahanshahi
Fully Patched Version: 2.9.8.6
Recommended Remediation: Update to version 2.9.8.6, or newer.
Publication Date: 2022-07-18

The Feed Them Social – for Twitter feed, Youtube and more plugin for WordPress is vulnerable to deserialization of untrusted input via the 'fts_url' parameter in versions up to, and including 2.9.8.5. This makes it possible for unauthenticated attackers to call files using a PHAR wrapper that will deserialize the data and call arbitrary PHP Objects that can be used to perform a variety of malicious actions granted a POP chain is also present. It also requires that the attacker is successful in uploading a file with the serialized payload.

AnyMind Widget <= 1.1 – Cross-Site Request Forgery to Cross-Site Scripting

Affected Plugin: AnyMind Widget
Plugin Slug: anymind-widget
Affected Versions: <= 1.2
CVE ID: CVE-2022-2435
CVSS Score: 8.8 (High)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
Researcher/s: Sho Sakata
Fully Patched Version: No patch available, plugin closed for download.
Recommended Remediation: Uninstall Plugin.
Publication Date: 2022-07-05

The AnyMind Widget plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including 1.1. This is due to missing nonce protection on the createDOMStructure() function found in the ~/anymind-widget-id.php file. This makes it possible for unauthenticated attackers to inject malicious web scripts into the page, granted they can trick a site's administrator into performing an action such as clicking on a link

FreeMind WP Browser <= 1.2 – Cross-Site Request Forgery to Cross-Site Scripting

Affected Plugin: FreeMind WP Browser
Plugin Slug: freemind-wp-browser
Affected Versions: <= 1.2
CVE ID: CVE-2022-2443
CVSS Score: 8.8 (High)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
Researcher/s: Kenya Uematsu
Fully Patched Version: No patch available, plugin closed for download.
Recommended Remediation: Uninstall Plugin.
Publication Date: 2022-07-05

The FreeMind WP Browser plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including 1.2. This is due to missing nonce protection on the FreemindOptions() function found in the ~/freemind-wp-browser.php file. This makes it possible for unauthenticated attackers to inject malicious web scripts into the page, granted they can trick a site's administrator into performing an action such as clicking on a link.

Visualizer: Tables and Charts Manager for WordPress <= 3.7.9 –

Affected Plugin: Visualizer: Tables and Charts Manager for WordPress
Plugin Slug: visualizer
Affected Versions: <= 3.7.9
CVE ID: CVE-2022-2444
CVSS Score: 8.8 (High)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
Researcher/s: Rasoul Jahanshahi
Fully Patched Version: 3.7.10
Recommended Remediation: Update to version 3.7.10, or newer.
Publication Date: 2022-07-05

The Visualizer: Tables and Charts Manager for WordPress plugin for WordPress is vulnerable to deserialization of untrusted input via the 'remote_data' parameter in versions up to, and including 3.7.9. This makes it possible for authenticated attackers with contributor privileges and above to call files using a PHAR wrapper that will deserialize the data and call arbitrary PHP Objects that can be used to perform a variety of malicious actions granted a POP chain is also present. It also requires that the attacker is successful in uploading a file with the serialized payload.

Import any XML or CSV File to WordPress <= 3.6.7 – Admin+ Malicious File Upload

Affected Plugin: Import any XML or CSV File to WordPress
Plugin Slug: wp-all-import
Affected Versions: <= 3.6.7
CVE ID: CVE-2022-1565
CVSS Score: 7.2 (Medium)
CVSS Vector: CVSS:3.1/A:H/I:H/C:H/S:U/UI:N/PR:H/AC:L/AV:N
Researcher/s: yangkang
Fully Patched Version: 3.6.8
Recommended Remediation: Update to version 3.6.8, or newer.
Publication Date: 2022-06-30

The plugin WP All Import is vulnerable to arbitrary file uploads due to missing file type validation via zip uploads in the wp_all_import_get_gz.php file in versions up to, and including, 3.6.7. This makes it possible for authenticated attackers, with administrator level permissions and above, to upload arbitrary files on the affected sites server which may make remote code execution possible.

Image Slider <= 1.1.121 – Cross-Site Request Forgery to Post Duplication

Affected Plugin: Image Slider
Plugin Slug: image-slider-widget
Affected Versions: <= 1.1.121
CVE ID: CVE-2022-2223
CVSS Score: 5.4 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N
Researcher/s: Marco Wotschka
Fully Patched Version: No patch available, plugin closed for download.
Recommended Remediation: Uninstall Plugin.
Publication Date: 2022-06-30

The WordPress plugin Image Slider is vulnerable to Cross-Site Request Forgery in versions up to, and including 1.1.121 due to failure to properly check for the existence of a nonce in the function ewic_duplicate_slider. This make it possible for unauthenticated attackers to duplicate existing posts or pages granted they can trick a site administrator into performing an action such as clicking on a link.

Gallery for Social Photo <= 1.0.0.27 – Cross-Site Request Forgery to Post Duplication

Affected Plugin: Gallery for Social Photo
Plugin Slug: feed-instagram-lite
Affected Versions: <= 1.0.0.27
CVE ID: CVE-2022-2224
CVSS Score: 5.4 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N
Researcher/s: Marco Wotschka
Fully Patched Version: No patch available, plugin closed for download.
Recommended Remediation: Uninstall Plugin.
Publication Date: 2022-06-30

The WordPress plugin Gallery for Social Photo is vulnerable to Cross-Site Request Forgery in versions up to, and including 1.0.0.27 due to failure to properly check for the existence of a nonce in the function gifeed_duplicate_feed. This make it possible for unauthenticated attackers to duplicate existing posts or pages granted they can trick a site administrator into performing an action such as clicking on a link.

Download Manager <= 3.2.46 – Contributor+ Cross-Site Scripting

Affected Plugin: Download Manager
Plugin Slug: download-manager
Affected Versions: <= 3.2.46
CVE ID: CVE-2022-2101
CVSS Score: 6.4 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:N
Researcher/s: Andrea Bocchetti
Fully Patched Version: 3.2.47
Recommended Remediation: Update to version 3.2.47, or newer.
Publication Date: 2022-06-30

The Download Manager plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the `file[files][]` parameter in versions up to, and including, 3.2.46 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers with contributor level permissions and above to inject arbitrary web scripts on the file's page that will execute whenever an administrator accesses the editor area for the injected file page. Read more here.

Free Live Chat Support <= 1.0.11 – Cross-Site Request Forgery to Cross-Site Scripting

Affected Plugin: Free Live Chat Support
Plugin Slug: livesupporti
Affected Versions: <= 1.0.11
CVE ID: CVE-2022-2039
CVSS Score: 8.8 (High)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
Researcher/s: Masaki Sunayama
Fully Patched Version: No patch available, plugin closed for download.
Recommended Remediation: Uninstall Plugin.
Publication Date: 2022-06-22

The Free Live Chat Support plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including 1.0.11. This is due to missing nonce protection on the livesupporti_settings() function found in the ~/livesupporti.php file. This makes it possible for unauthenticated attackers to inject malicious web scripts into the page, granted they can trick a site's administrator into performing an action such as clicking on a link.

DX Share Selection <= 1.4 – Cross-Site Request Forgery to Cross-Site Scripting

Affected Plugin: DX Share Selection
Plugin Slug: dx-share-selection
Affected Versions: <= 1.4
CVE ID: CVE-2022-2001
CVSS Score: 8.8 (High)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
Researcher/s: Sho Sakata
Fully Patched Version: No patch available, plugin closed for download.
Recommended Remediation: Uninstall Plugin.
Publication Date: 2022-06-22

The DX Share Selection plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including 1.4. This is due to missing nonce protection on the dxss_admin_page() function found in the ~/dx-share-selection.php file. This makes it possible for unauthenticated attackers to inject malicious web scripts into the page, granted they can trick a site's administrator into performing an action such as clicking on a link.

GiveWP – Donation Plugin and Fundraising Platform – 2.20.2

Affected Plugin: GiveWP – Donation Plugin and Fundraising Platform
Plugin Slug: give
Affected Versions: <= 2.20.2
CVE ID: CVE-2022-2117
CVSS Score: 5.3 (Medium)
CVSS Vector: CVSS:3.1/A:N/I:N/C:L/S:U/UI:N/PR:N/AC:L/AV:N
Researcher/s: Kane Gamble (Blackfoot UK)
Fully Patched Version: 2.21.0
Recommended Remediation: Update to version 2.21.0, or newer.
Publication Date: 2022-06-17

The GiveWP plugin for WordPress is vulnerable to Sensitive Information Disclosure in versions up to, and including, 2.20.2 via the /donor-wall REST-API endpoint which provides unauthenticated users with donor information even when the donor wall is not enabled. This functionality has been completely removed in version 2.20.2.

Wbcom Designs – BuddyPress Group Reviews <= 2.8.3 – Unauthorized AJAX Actions due to Nonce Bypass

Affected Plugin: Wbcom Designs – BuddyPress Group Reviews
Plugin Slug: review-buddypress-groups
Affected Versions: <= 2.8.3
CVE ID: CVE-2022-2108
CVSS Score: 8.8 (High)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
Researcher/s: Marco Wotschka, Wordfence
Fully Patched Version: 2.8.4
Recommended Remediation: Update to version 2.8.4, or newer.
Publication Date: 2022-06-16

The plugin Wbcom Designs – BuddyPress Group Reviews for WordPress is vulnerable to unauthorized settings changes and review modification due to missing capability checks and improper nonce checks in several functions related to said actions in versions up to, and including, 2.8.3. This makes it possible for unauthenticated attackers to modify reviews and plugin settings on the affected site.

Button Widget Smartsoft <= 1.0.1 – Cross-Site Request Forgery to Cross-Site Scripting

Affected Plugin: Button Widget Smartsoft
Plugin Slug: smartsoftbutton-widget-de-botones-de-chat
Affected Versions: <= 1.0.1
CVE ID: CVE-2022-1912
CVSS Score: 8.8 (High)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
Researcher/s: Ryo Onodera, Cryptography Laboratory in Tokyo Denki University
Fully Patched Version: No patch available, plugin closed for download.
Recommended Remediation: Uninstall Plugin.
Publication Date: 2022-06-16

The Button Widget Smartsoft plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.0.1. This is due to missing nonce validation on the smartsoftbutton_settings page. This makes it possible for unauthenticated attackers to update the plugins settings and inject malicious web scripts via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.

Mitsol Social Post Feed <= 1.10 – Authenticated (Admin+) Stored Cross-Site Scripting

Affected Plugin: Mitsol Social Post Feed
Plugin Slug: facebook-wall-and-social-integration
Affected Versions: <= 1.10
CVE ID: CVE-2022-0209
CVSS Score: 5.5 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:L/I:L/A:N
Researcher/s: Big Tiger
Fully Patched Version: No patch available, plugin closed for download.
Recommended Remediation: Uninstall Plugin.
Publication Date: 2022-06-10

The Mitsol Social Post Feed plugin for WordPress is vulnerable to Stored Cross-Site Scripting in versions up to, and including, 1.10 due to insufficient input sanitization and output escaping on the application id parameters. This makes it possible for authenticated (admin+) attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html is disabled.

ToolBar to Share <= 2.0 – Cross-Site Request Forgery to Cross-Site Scripting

Affected Plugin: ToolBar to Share
Plugin Slug: toolbar-to-share
Affected Versions: <= 2.0
CVE ID: CVE-2022-1918
CVSS Score: 8.8 (High)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
Researcher/s: Sho Sakata, Cryptography Laboratory in Tokyo Denki University
Fully Patched Version: No patch available, plugin closed for download.
Recommended Remediation: Uninstall Plugin.
Publication Date: 2022-06-09

The ToolBar to Share plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 2.0. This is due to missing nonce validation on the plugin_toolbar_comparte page. This makes it possible for unauthenticated attackers to update the plugins settings and inject malicious web scripts via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.

Copify <= 1.3.0 – Cross-Site Request Forgery to Cross-Site Scripting

Affected Plugin: Copify
Plugin Slug: copify
Affected Versions: <= 1.3.0
CVE ID: CVE-2022-1900
CVSS Score: 8.8 (High)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
Researcher/s: Yuki Hoshi, Cryptography Laboratory in Tokyo Denki University
Fully Patched Version: No patch available, plugin closed for download.
Recommended Remediation: Uninstall Plugin.
Publication Date: 2022-06-08

The Copify plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.3.0. This is due to missing nonce validation on the CopifySettings page. This makes it possible for unauthenticated attackers to update the plugins settings and inject malicious web scripts via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.

Download Manager <= 3.2.42 – Reflected Cross-Site Scripting

Affected Plugin: Download Manager
Plugin Slug: download-manager
Affected Versions: <= 3.2.42
CVE ID: CVE-2022-1985
CVSS Score: 6.1 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
Researcher/s: Rafie Muhammad (Yeraisci)
Fully Patched Version: 3.2.43
Recommended Remediation: Update to version 3.2.43, or newer.
Publication Date: 2022-06-02

The Download Manager Plugin for WordPress is vulnerable to reflected Cross-Site Scripting in versions up to, and including 3.2.42. This is due to insufficient input sanitization and output escaping on the 'frameid' parameter found in the ~/src/Package/views/shortcode-iframe.php file.

Ultimate Member <= 2.3.2 – Stored Cross-Site Scripting

Affected Versions: <= 2.3.2
CVE ID: CVE-2022-1208
CVSS Score: 6.4 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:N
Researcher/s: Ruijie Li
Fully Patched Version: 2.4.0
Recommended Remediation: Update to version 2.4.0, or newer.
Publication Date: 2022-06-02

The Ultimate Member plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Biography field featured on individual user profile pages due to insufficient input sanitization and output escaping that allows users to encode malicious web scripts with HTML encoding that is reflected back on the page. This affects versions up to, and including, 2.3.2. Please note this issue was only partially fixed in version 2.3.2.

Mobile browser color select <= 1.0.1 – Cross-Site Request Forgery to Stored Cross-Site Scripting

Affected Plugin: Mobile browser color select
Plugin Slug: mobile-browser-color-select
Affected Versions: <= 1.0.1
CVE ID: CVE-2022-1969
CVSS Score: 8.8 (High)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
Researcher/s: Tsubasa Imaizumi, Cryptography Laboratory in Tokyo Denki University
Fully Patched Version: No patch available, plugin closed for download.
Recommended Remediation: Uninstall Plugin.
Publication Date: 2022-06-01

The Mobile browser color select plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.0.1. This is due to missing or incorrect nonce validation on the admin_update_data() function. This makes it possible for unauthenticated attackers to inject malicious web scripts via forged request granted they can trick a site administrator into performing an action such as clicking on a link.

Google Tag Manager for WordPress (GTM4WP) <= 1.15.1 – Stored Cross-Site Scripting via Content Element ID

Affected Plugin: Google Tag Manager for WordPress (GTM4WP)
Plugin Slug: duracelltomi-google-tag-manager
Affected Versions: <= 1.15.1
CVE ID: CVE-2022-1961
CVSS Score: 5.5 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:L/I:L/A:N
Researcher/s: Muhammad Zeeshan (Xib3rR4dAr)
Fully Patched Version: 1.15.2
Recommended Remediation: Update to version 1.15.2, or newer.
Publication Date: 2022-05-31

The Google Tag Manager for WordPress plugin is vulnerable to Stored Cross-Site Scripting due to insufficient escaping via the `gtm4wp-options[scroller-contentid]` parameter found in the `~/public/frontend.php` file which allowed attackers with administrative user access to inject arbitrary web scripts, in versions up to and including 1.15.1. This affects multi-site installations where unfiltered_html is disabled for administrators, and sites where unfiltered_html is disabled.

WPMK Ajax Finder <= 1.0.1 – Cross-Site Request Forgery to Cross-Site Scripting

Affected Plugin: WPMK Ajax Finder
Plugin Slug: find-any-think
Affected Versions: <= 1.0.1
CVE ID: CVE-2022-1749
CVSS Score: 8.8 (High)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
Researcher/s: Tsubasa Imaizumi, Cryptography Laboratory in Tokyo Denki University
Fully Patched Version: No patch available, plugin closed for download.
Recommended Remediation: Uninstall Plugin.
Publication Date: 2022-05-31

The WPMK Ajax Finder WordPress plugin is vulnerable to Cross-Site Request Forgery via the createplugin_atf_admin_setting_page() function found in the ~/inc/config/create-plugin-config.php file due to a missing nonce check which allows attackers to inject arbitrary web scripts, in versions up to and including 1.0.1.

Zephyr Project Manager <= 3.2.40 – Reflected Cross-Site Scripting

Affected Plugin: Zephyr Project Manager
Plugin Slug: zephyr-project-manager
Affected Versions: <= 3.2.40
CVE ID: CVE-2022-1822
CVSS Score: 6.1 (Medium)
CVSS Vector: CVSS:3.1/A:N/I:L/C:L/S:C/UI:R/PR:N/AC:L/AV:N
Researcher/s: Eduardo Estevao de Oliveira Azevedo
Fully Patched Version: 3.2.41
Recommended Remediation: Update to version 3.2.41, or newer.
Publication Date: 2022-05-23

The Zephyr Project Manager plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'project' parameter in versions up to, and including, 3.2.40 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.

Keep Backup Daily <= 2.0.2 – Reflected Cross-Site Scripting

Affected Plugin: Keep Backup Daily
Plugin Slug: keep-backup-daily
Affected Versions: <= 2.0.2
CVE ID: CVE-2022-1820
CVSS Score: 6.1 (Medium)
CVSS Vector: CVSS:3.1/A:N/I:L/C:L/S:C/UI:R/PR:N/AC:L/AV:N
Researcher/s: Eduardo Estevao de Oliveira Azevedo
Fully Patched Version: 2.0.3
Recommended Remediation: Update to version 2.0.3, or newer.
Publication Date: 2022-05-23

The Keep Backup Daily plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 't' parameter in versions up to, and including, 2.0.2 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.

Sticky Popup <= 1.2 – Admin+ Stored Cross-Site Scripting

Affected Plugin: Sticky Popup
Plugin Slug: sticky-popup
Affected Versions: <= 1.2
CVE ID: CVE-2022-1750
CVSS Score: 5.5 (Medium)
CVSS Vector: CVSS:3.1/A:N/I:L/C:L/S:C/UI:N/PR:H/AC:L/AV:N
Researcher/s: Saeed Alzahrani
Fully Patched Version: No patch available, plugin closed for download.
Recommended Remediation: Uninstall Plugin.
Publication Date: 2022-05-23

The Sticky Popup plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the '`popup_title`' parameter in versions up to, and including, 1.2 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with admin level capabilities and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This issue mostly affects sites where `unfiltered_html` has been disabled for administrators and on multi-site installations where `unfiltered_html` is disabled for administrators.

Google Tag Manager for WordPress <= 1.15 – Reflected Cross-Site

Affected Plugin: Google Tag Manager for WordPress
Plugin Slug: duracelltomi-google-tag-manager
Affected Versions: <= 1.15
CVE ID: CVE-2022-1707
CVSS Score: 6.1 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
Researcher/s: Cory Buecker & not_stoppable
Fully Patched Version: 1.15.1
Recommended Remediation: Update to version 1.15.1, or newer.
Publication Date: 2022-05-19

The Google Tag Manager for WordPress plugin for WordPress is vulnerable to reflected Cross-Site Scripting via the s parameter due to the site search populating into the data layer of sites in versions up to an including 1.15. The affected file is ~/public/frontend.php and this could be exploited by unauthenticated attackers.

RSVPMaker <= 9.3.2 – Unauthenticated SQL Injection

Affected Plugin: RSVPMaker
Plugin Slug: rsvpmaker
Affected Versions: <= 9.3.2
CVE ID: CVE-2022-1768
CVSS Score: 9.8 (Critical)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Researcher/s: Muhammad Zeeshan (Xib3rR4dAr)
Fully Patched Version: 9.3.3
Recommended Remediation: Update to version 9.3.3, or newer.
Publication Date: 2022-05-17

The RSVPMaker plugin for WordPress is vulnerable to unauthenticated SQL Injection due to insufficient escaping and parameterization on user supplied data passed to multiple SQL queries in the ~/rsvpmaker-email.php file. This makes it possible for unauthenticated attackers to steal sensitive information from the database in versions up to, and including, 9.3.2. Please note that this is separate from CVE-2022-1453 & CVE-2022-1505.

WP JS <= 2.0.6 – Reflected Cross-Site Scripting

Affected Plugin: WP JS
Plugin Slug: wp-js
Affected Versions: <= 2.0.6
CVE ID: CVE-2022-1567
CVSS Score: 6.1 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
Researcher/s: Marco Wotschka
Fully Patched Version: No patch available, plugin closed for download.
Recommended Remediation: Uninstall Plugin.
Publication Date: 2022-05-03

The WP-JS plugin for WordPress contains a script called wp-js.php with the function `wp_js_admin`, that accepts unvalidated user input and echoes it back to the user. This can be used for reflected Cross-Site Scripting in versions up to, and including, 2.0.6.

Ultimate Member – User Profile, User Registration, Login & Membership Plugin <= 2.3.1 – Open Redirect

Affected Plugin: Ultimate Member – User Profile, User Registration, Login & Membership Plugin
Plugin Slug: ultimate-member
Affected Versions: <= 2.3.1
CVE ID: CVE-2022-1209
CVSS Score: 4.3 (Medium)
CVSS Vector: CVSS:3.1/A:N/I:L/C:N/S:U/UI:R/PR:N/AC:L/AV:N
Researcher/s: Rujjie Li
Fully Patched Version: 2.3.2
Recommended Remediation: Update to version 2.3.2, or newer.
Publication Date: 2022-04-29

The Ultimate Member plugin for WordPress is vulnerable to arbitrary redirects due to insufficient validation on supplied URLs in the social fields of the Profile Page, which makes it possible for attackers to redirect unsuspecting victims in versions up to, and including, 2.3.1.

All-in-One WP Migration <=7.58 – Directory Traversal to File Deletion on Windows Hosts

Affected Plugin: All-in-One WP Migration
Plugin Slug: all-in-one-wp-migration
Affected Versions: <= 7.58
CVE ID: CVE-2022-1476
CVSS Score: 6.6 (Medium)
CVSS Vector: CVSS:3.1/A:H/I:H/C:H/S:U/UI:N/PR:H/AC:H/AV:N
Researcher/s: haidv35 from Viettel Cyber Security
Fully Patched Version: 7.59
Recommended Remediation: Update to version 7.59, or newer.
Publication Date: 2022-04-28

The All-in-One WP Migration plugin for WordPress is vulnerable to arbitrary file deletion via directory traversal due to insufficient file validation via the ~/lib/model/class-ai1wm-backups.php file, in versions up to, and including, 7.58. This can be exploited by administrative users, and users who have access to the site's secret key on WordPress instances with Windows hosts.

RSVPMaker <= 9.2.6 – Unauthenticated SQL Injection

Affected Plugin: RSVPMaker
Plugin Slug: rsvpmaker
Affected Versions: <= 9.2.6
CVE ID: CVE-2022-1505
CVSS Score: 9.8 (Critical)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Researcher/s: Tobias Kay Dalå (oxnan)
Fully Patched Version: 9.2.7
Recommended Remediation: Update to version 9.2.7, or newer.
Publication Date: 2022-04-27

The RSVPMaker plugin for WordPress is vulnerable to unauthenticated SQL Injection due to missing SQL escaping and parameterization on user supplied data passed to a SQL query in the rsvpmaker-api-endpoints.php file. This makes it possible for unauthenticated attackers to steal sensitive information from the database in versions up to, and including, 9.2.6.

RSVPMaker <= 9.2.5 – Unauthenticated SQL Injection

Affected Plugin: RSVPMaker
Plugin Slug: rsvpmaker
Affected Versions: <= 9.2.5
CVE ID: CVE-2022-1453
CVSS Score: 9.8 (Critical)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Researcher/s: Tobias Kay Dalå (oxnan)
Fully Patched Version: 9.2.6
Recommended Remediation: Update to version 9.2.6, or newer.
Publication Date: 2022-04-26

The RSVPMaker plugin for WordPress is vulnerable to unauthenticated SQL Injection due to missing SQL escaping and parameterization on user supplied data passed to a SQL query in the rsvpmaker-util.php file. This makes it possible for unauthenticated attackers to steal sensitive information from the database in versions up to, and including, 9.2.5.

Metform Elementor Contact Form Builder <= 2.1.3 – Sensitive Information Disclosure

Affected Plugin: Metform Elementor Contact Form Builder
Plugin Slug: metform
Affected Versions: <= 2.1.3
CVE ID: CVE-2022-1442

CVSS Score: 7.5 (High)
CVSS Vector: CVSS:3.1/A:N/I:N/C:H/S:U/UI:N/PR:N/AC:L/AV:N

Publication Date: 2022-04-23

The Metform WordPress plugin is vulnerable to sensitive information disclosure due to improper access control in the ~/core/forms/action.php file which can be exploited by an unauthenticated attacker to view all API keys and secrets of integrated third-party APIs like that of PayPal, Stripe, Mailchimp, Hubspot, HelpScout, reCAPTCHA and many more, in versions up to and including 2.1.3.

Fancy Product Designer <= 4.7.5 – Cross-Site Request Forgery to Arbitrary File Upload

Affected Plugin: Fancy Product Designer
Plugin Slug: fancy-product-designer
Affected Versions: <= 4.7.5
CVE ID: CVE-2021-4096
CVSS Score: 8.8 (High)
CVSS Vector: CVSS:3.1/A:H/I:H/C:H/S:U/UI:R/PR:N/AC:L/AV:N
Researcher/s: Lin Yu
Fully Patched Version: 4.7.6
Recommended Remediation: Update to version 4.7.6, or newer.
Publication Date: 2022-04-14

The Fancy Product Designer plugin for WordPress is vulnerable to Cross-Site Request Forgery via the FPD_Admin_Import class that makes it possible for attackers to upload malicious files that could be used to gain webshell access to a server in versions up to, and including, 4.7.5.

WP YouTube Live <= 1.7.21 – Reflected Cross-Site Scripting

Affected Plugin: WP YouTube Live
Plugin Slug: wp-youtube-live
Affected Versions: <= 1.7.21
CVE ID: CVE-2022-1187
CVSS Score: 5.4 (Medium)
CVSS Vector: CVSS:3.1/A:N/I:L/C:L/S:C/UI:R/PR:L/AC:L/AV:N
Researcher/s: p764
Fully Patched Version: 1.7.22
Recommended Remediation: Update to version 1.7.22, or newer.
Publication Date: 2022-03-31

The WordPress WP YouTube Live Plugin is vulnerable to Reflected Cross-Site Scripting via POST data found in the ~/inc/admin.php file which allows unauthenticated attackers to inject arbitrary web scripts in versions up to, and including, 1.7.21.

Be POPIA Compliant <= 1.1.5 – Sensitive Information Exposure

Affected Plugin: Be POPIA Compliant
Plugin Slug: be-popia-compliant
Affected Versions: <= 1.1.5
CVE ID: CVE-2022-1186
CVSS Score: 5.3 (Medium)
CVSS Vector: CVSS:3.1/A:N/I:N/C:L/S:U/UI:N/PR:N/AC:L/AV:N
Researcher/s: Chris Meistre
Fully Patched Version: 1.1.6
Recommended Remediation: Update to version 1.1.6, or newer.
Publication Date: 2022-03-30

The WordPress plugin Be POPIA Compliant exposed sensitive information to unauthenticated users consisting of site visitors emails and usernames via an API route, in versions up to an including 1.1.5.

Simple File List <= 3.2.7 – Arbitrary File Download

Affected Plugin: Simple File List
Plugin Slug: simple-file-list
Affected Versions: <= 3.2.7
CVE ID: CVE-2022-1119
CVSS Score: 7.5 (High)
CVSS Vector: CVSS:3.1/A:N/I:N/C:H/S:U/UI:N/PR:N/AC:L/AV:N
Researcher/s: Admavidhya N
Reporter: Bernardo Rodrigues
Fully Patched Version: 3.2.8
Recommended Remediation: Update to version 3.2.8, or newer.
Publication Date: 2022-03-28

The Simple File List WordPress plugin is vulnerable to Arbitrary File Download via the `eeFile` parameter found in the ~/includes/ee-downloader.php file due to missing controls which makes it possible unauthenticated attackers to supply a path to a file that will subsequently be downloaded, in versions up to and including 3.2.7.

Ninja Forms – File Uploads Extension <= 3.3.0 Arbitrary File Upload

Affected Plugin: Ninja Forms – File Uploads Extension
Plugin Slug: ninja-forms-uploads
Affected Versions: <= 3.3.0
CVE ID: CVE-2022-0888
CVSS Score: 9.8 (Critical)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Reporter: Muhammad Zeeshan (Xib3rR4dAr)
Fully Patched Version: 3.3.1
Recommended Remediation: Update to version 3.3.1, or newer.
Publication Date: 2022-03-08

The Ninja Forms – File Uploads Extension WordPress plugin is vulnerable to arbitrary file uploads due to insufficient input file type validation found in the ~/includes/ajax/controllers/uploads.php file which can be bypassed making it possible for unauthenticated attackers to upload malicious files that can be used to obtain remote code execution, in versions up to and including 3.3.0

Ninja Forms – File Uploads Extension <= 3.3.12 Reflected Cross-Site Scripting

Affected Plugin: Ninja Forms – File Uploads Extension
Plugin Slug: ninja-forms-uploads
Affected Versions: <= 3.3.12
CVE ID: CVE-2022-0889
CVSS Score: 6.1(Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
Researcher/s: Nuno Correia (Blaze Security)
Reporter: Muhammad Zeeshan (Xib3rR4dAr)
Fully Patched Version: 3.3.13
Recommended Remediation: Update to version 3.3.13, or newer.
Publication Date: 2022-03-08

The Ninja Forms – File Uploads Extension WordPress plugin is vulnerable to reflected cross-site scripting due to missing sanitization of the files filename parameter found in the ~/includes/ajax/controllers/uploads.php file which can be used by unauthenticated attackers to add malicious web scripts to vulnerable WordPress sites, in versions up to and including 3.3.12.

Amelia <= 1.0.46 Stored Cross Site Scripting via lastName

Affected Plugin: Amelia
Plugin Slug: ameliabooking
Affected Versions: <= 1.0.46
CVE ID: CVE-2022-0834
CVSS Score: 7.2 (High)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:L/A:N
Researcher/s: Vinay Kumar from Trellix
Fully Patched Version: 1.0.47
Recommended Remediation: Update to version 1.0.47, or newer.
Publication Date: 2022-03-02

The Amelia WordPress plugin is vulnerable to Cross-Site Scripting due to insufficient escaping and sanitization of the `lastName` parameter found in the ~/src/Application/Controller/User/Customer/AddCustomerController.php file which allows attackers to inject arbitrary web

Essential Addons for Elementor Lite <= 5.0.8 Reflected Cross-Site Scripting

Affected Plugin: Essential Addons for Elementor Lite
Plugin Slug: essential-addons-for-elementor-lite
Affected Versions: <=5.0.8
CVE ID: CVE-2022-0633
CVSS Score: 6.1 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
Researcher/s: Pham Van Khanh (rskvp93) from VCSLab of Viettel Cyber Security & Nguyen Dinh Bien (biennd4) from VCSLab of Viettel Cyber Security.
Fully Patched Version: 5.0.9
Recommended Remediation: Update to version 5.0.9, or newer.
Publication Date: 2022-02-18

The Essential Addons for Elementor Lite WordPress plugin is vulnerable to Cross-Site Scripting due to insufficient escaping and sanitization of the `settings` parameter found in the ~/includes/Traits/Helper.php file which allows attackers to inject arbitrary web scripts onto a pages that executes whenever a user clicks on a specially crafted link by an attacker. This affects versions up to and including 5.0.8.

WP Statistics <= 13.1.5 Unauthenticated Stored Cross-Site Scripting via IP

Affected Plugin: WP Statistics
Plugin Slug: wp-statistics
Affected Versions: <=13.1.5
CVE ID: CVE-2022-25305
CVSS Score: 7.2 (High)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:L/A:N
Researcher/s: Muhammad Zeeshan (Xib3rR4dAr)
Fully Patched Version: 13.1.6
Recommended Remediation: Update to version 13.1.6, or newer.
Publication Date: 2022-02-17

The WP Statistics WordPress plugin is vulnerable to Cross-Site Scripting due to insufficient escaping and sanitization of the `IP` parameter found in the ~/includes/class-wp-statistics-hits.php file which allows attackers to inject arbitrary web scripts onto several pages that execute when site administrators view a sites statistics, in versions up to and including 13.1.5.

WP Statistics <= 13.1.5 Unauthenticated Stored Cross-Site Scripting via browser

Affected Plugin: WP Statistics
Plugin Slug: wp-statistics
Affected Versions: <=13.1.5
CVE ID: CVE-2022-25306
CVSS Score: 7.2 (High)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:L/A:N
Researcher/s: Muhammad Zeeshan (Xib3rR4dAr)
Fully Patched Version: 13.1.6
Recommended Remediation: Update to version 13.1.6, or newer.
Publication Date: 2022-02-17

The WP Statistics WordPress plugin is vulnerable to Cross-Site Scripting due to insufficient escaping and sanitization of the `browser` parameter found in the ~/includes/class-wp-statistics-hits.php file which allows attackers to inject arbitrary web scripts onto several pages that execute when site administrators view a sites statistics, in versions up to and including 13.1.5.

WP Statistics <= 13.1.5 Unauthenticated Stored Cross-Site Scripting via platform

Affected Plugin: WP Statistics
Plugin Slug: wp-statistics
Affected Versions: <=13.1.5
CVE ID: CVE-2022-25307
CVSS Score: 7.2 (High)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:L/A:N
Researcher/s: Muhammad Zeeshan (Xib3rR4dAr)
Fully Patched Version: 13.1.6
Recommended Remediation: Update to version 13.1.6, or newer.
Publication Date: 2022-02-17

The WP Statistics WordPress plugin is vulnerable to Cross-Site Scripting due to insufficient escaping and sanitization of the `platform` parameter found in the ~/includes/class-wp-statistics-hits.php file which allows attackers to inject arbitrary web scripts onto several pages that execute when site administrators view a sites statistics, in versions up to and including 13.1.5.

WP Statistics <= 13.1.5 Unauthenticated Blind SQL Injection via current_page_id

Affected Plugin: WP Statistics
Plugin Slug: wp-statistics
Affected Versions: <=13.1.5
CVE ID: CVE-2022-25148
CVSS Score: 9.8 (Critical)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Researcher/s: Muhammad Zeeshan (Xib3rR4dAr)
Fully Patched Version: 13.1.6
Recommended Remediation: Update to version 13.1.6, or newer.
Publication Date: 2022-02-16

The WP Statistics WordPress plugin is vulnerable to SQL Injection due to insufficient escaping and parameterization of the `current_page_id` parameter found in the ~/includes/class-wp-statistics-hits.php file which allows attackers without authentication to inject arbitrary SQL queries to obtain sensitive information, in versions up to and including 13.1.5.

WP Statistics <= 13.1.5 Unauthenticated Blind SQL Injection via IP

Affected Plugin: WP Statistics
Plugin Slug: wp-statistics
Affected Versions: <=13.1.5
CVE ID: CVE-2022-25149
CVSS Score: 9.8 (Critical)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Researcher/s: Muhammad Zeeshan (Xib3rR4dAr)
Fully Patched Version: 13.1.6
Recommended Remediation: Update to version 13.1.6, or newer.
Publication Date: 2022-02-16

The WP Statistics WordPress plugin is vulnerable to SQL Injection due to insufficient escaping and parameterization of the `IP` parameter found in the ~/includes/class-wp-statistics-hits.php file which allows attackers without authentication to inject arbitrary SQL queries to obtain sensitive information, in versions up to and including 13.1.5.

WP Statistics <= 13.1.5 Unauthenticated Blind SQL Injection via current_page_type

Affected Plugin: WP Statistics
Plugin Slug: wp-statistics
Affected Versions: <=13.1.5
CVE ID: CVE-2022-0651
CVSS Score: 9.8 (Critical)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Researcher/s: Muhammad Zeeshan (Xib3rR4dAr)
Fully Patched Version: 13.1.6
Recommended Remediation: Update to version 13.1.6, or newer.
Publication Date: 2022-02-16

The WP Statistics WordPress plugin is vulnerable to SQL Injection due to insufficient escaping and parameterization of the `current_page_type` parameter found in the ~/includes/class-wp-statistics-hits.php file which allows attackers without authentication to

WP Statistics <= 13.1.4 Unauthenticated Blind SQL Injection via exclusion_reason

Affected Plugin: WP Statistics
Plugin Slug: wp-statistics
Affected Versions: <=13.1.4
CVE ID: CVE-2022-0513
CVSS Score: 9.8 (Critical)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Researcher/s: Cyku Hong from DEVCORE
Fully Patched Version: 13.1.5
Recommended Remediation: Update to version 13.1.5, or newer.
Publication Date: 2022-02-10

The WP Statistics WordPress plugin is vulnerable to SQL Injection due to insufficient escaping and parameterization of the `exclusion_reason` parameter found in the ~/includes/class-wp-statistics-exclusion.php file which allows attackers without authentication to inject arbitrary SQL queries to obtain sensitive information, in versions up to and including 13.1.4. This requires the "Record Exclusions" option to be enabled on the vulnerable site. Read more here.

PHP Everywhere <= 2.0.3 Remote Code Execution via Gutenberg blocks

Affected Plugin: PHP Everywhere
Plugin Slug: php-everywhere
Affected Versions: <= 2.0.3
CVE ID: CVE-2022-24665
CVSS Score: 9.9 (Critical)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H
Researcher/s: Ramuel Gall
Fully Patched Version: 3.0.0
Recommended Remediation: Update to version 3.0.0, or newer.
Publication Date: 2022-02-08

PHP Everywhere <= 2.0.3 included functionality that allowed execution of PHP Code Snippets via a gutenberg block, which could be used by any user able to edit posts. Read more here.

PHP Everywhere <= 2.0.3 Remote Code Execution via metabox

Affected Plugin: PHP Everywhere
Plugin Slug: php-everywhere
Affected Versions: <= 2.0.3
CVE ID: CVE-2022-24664
CVSS Score: 9.9 (Critical)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H
Researcher/s: Ramuel Gall
Fully Patched Version: 3.0.0
Recommended Remediation: Update to version 3.0.0, or newer.
Publication Date: 2022-02-08

PHP Everywhere <= 2.0.3 included functionality that allowed execution of PHP Code Snippets via WordPress metabox, which could be used by any user able to edit posts. Read more here.

PHP Everywhere <= 2.0.3 Remote Code Execution via shortcode

Affected Plugin: PHP Everywhere
Plugin Slug: php-everywhere
Affected Versions: <= 2.0.3
CVE ID: CVE-2022-24663
CVSS Score: 9.9 (Critical)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H
Researcher/s: Ramuel Gall
Fully Patched Version: 3.0.0
Recommended Remediation: Update to version 3.0.0, or newer.
Publication Date: 2022-02-08

PHP Everywhere <= 2.0.3 included functionality that allowed execution of PHP Code Snippets via WordPress shortcodes, which can be used by any authenticated user. Read more here.

Fancy Product Designer <= 4.7.4 Admin+ SQL Injection

Affected Plugin: Fancy Product Designer
Plugin Slug: fancy-product-designer
Affected Versions: <= 4.7.4
CVE ID: CVE-2021-4134
CVSS Score: 7.2 (High)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H
Researcher/s: Lin Yu
Fully Patched Version: 4.7.5
Recommended Remediation: Update to version 4.7.5, or newer.
Publication Date: 2022-02-08

The Fancy Product Designer WordPress plugin is vulnerable to SQL Injection due to insufficient escaping and parameterization of the `id` parameter found in the ~/inc/api/class-view.php file which allows attackers with administrative level permissions to inject arbitrary SQL queries to obtain sensitive information, in versions up to and including 4.7.4.

Fotobook <= 3.2.3 Reflected Cross-Site Scripting

Affected Plugin: Fotobook
Plugin Slug: fotobook
Affected Versions: <= 3.2.3
CVE ID: CVE-2022-03801
CVSS Score: 6.1 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
Researcher/s: p7e4
Fully Patched Version: No patch available, plugin closed for download.
Recommended Remediation: Uninstall Plugin.
Publication Date: 2022-01-31

The Fotobook WordPress plugin is vulnerable to Reflected Cross-Site Scripting due to insufficient escaping and the use of `$_SERVER['PHP_SELF']` found in the ~/options-fotobook.php file which allows attackers to inject arbitrary web scripts onto the page, in versions up to and including 3.2.3.

Embed Swagger <= 1.0.0 Reflected Cross-Site Scripting

Affected Plugin: Embed Swagger
Plugin Slug: embed-swagger
Affected Versions: <= 1.0.0
CVE ID: CVE-2022-0381
CVSS Score: 6.1 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
Researcher/s: Muhammad Zeeshan (Xib3rR4dAr)
Fully Patched Version: No patch available, plugin closed for download.
Recommended Remediation: Uninstall Plugin.
Publication Date: 2022-01-26

The Embed Swagger WordPress plugin is vulnerable to Reflected Cross-Site Scripting due to insufficient escaping/sanitization and validation via the `url` parameter found in the ~/swagger-iframe.php file which allows attackers to inject arbitrary web scripts onto the page, in versions up to and including 1.0.0.

ProfileGrid – User Profiles, Memberships, Groups and Communities <= 4.7.4 Authenticated Stored Cross-Site Scripting

Affected Plugin: ProfileGrid – User Profiles, Memberships, Groups and Communities
Plugin Slug: profilegrid-user-profiles-groups-and-communities

Affected Versions: <= 4.7.4
CVE ID: CVE-2022-0233

Fully Patched Version: No patch available, plugin closed for download.
Recommended Remediation: Uninstall Plugin.
Publication Date: 2022-01-18

The ProfileGrid – User Profiles, Memberships, Groups and Communities WordPress plugin is vulnerable to Stored Cross-Site Scripting due to insufficient escaping via the `pm_user_avatar` and `pm_cover_image` parameters found in the ~/admin/class-profile-magic-admin.php file which allows attackers with authenticated user access, such as subscribers, to inject arbitrary web scripts into their profile, in versions up to and including 1.2.7.

User Registration, Login & Landing Pages – LeadMagic <= 1.2.7 Admin+ Stored Cross-Site Scripting

Affected Plugin: User Registration, Login & Landing Pages – LeadMagic
Plugin Slug: custom-landing-pages-leadmagic
Affected Versions: <= 1.2.7
CVE ID: CVE-2022-0232
CVSS Score: 4.8 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:C/C:L/I:L/A:N
Researcher/s: Big Tiger
Fully Patched Version: No patch available, plugin closed for download.
Recommended Remediation: Uninstall Plugin.
Publication Date: 2022-01-18

The User Registration, Login & Landing Pages WordPress plugin is vulnerable to Stored Cross-Site Scripting due to insufficient escaping via the `loader_text` parameter found in the ~/includes/templates/landing-page.php file which allows attackers with administrative user access to inject arbitrary web scripts, in versions up to and including 1.2.7. This affects multi-site installations where `unfiltered_html` is disabled for administrators, and sites where `unfiltered_html` is disabled.

WP Import Export Lite & WP Import Export <= 3.9.15 Unauthenticated Sensitive Data Disclosure

Affected Plugin: WP Import Export Lite & WP Import Export
Plugin Slug: wp-import-export-lite & wp-import-export
Affected Versions: <= 3.9.15
CVE ID: CVE-2022-0236
CVSS Score: 7.5 (High)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
Researcher/s: Karan Saini (Kloudle Inc.)
Fully Patched Version: 3.9.16
Recommended Remediation: Update to version 3.9.16, or newer.
Publication Date: 2022-01-14

The WP Import Export WordPress plugin (both free and premium versions) is vulnerable to unauthenticated sensitive data disclosure due to a missing capability check on the download function `wpie_process_file_download` found in the ~/includes/classes/class-wpie-general.php file. This made it possible for unauthenticated attackers to download any imported or exported information from a vulnerable site which can contain sensitive information like user data. This affects versions up to, and including, 3.9.15.

WHMCS Bridge <= 6.1 Subscriber+ Stored Cross-Site Scripting

Affected Plugin: WHMCS Bridge
Plugin Slug: whmcs-bridge
Affected Versions: <= 6.1
CVE ID: CVE-2021-4074
CVSS Score: 6.4 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:N
Researcher/s: Kazuto Kokonoe, Tokyo Denki University Cryptography Laboratory
Fully Patched Version: 6.3
Recommended Remediation: Update to version 6.3, or newer.
Publication Date: 2022-01-14

The WHMCS Bridge WordPress plugin is vulnerable to Stored Cross-Site Scripting via the `cc_whmcs_bridge_url` parameter found in the ~/whmcs-bridge/bridge_cp.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 6.1. Due to missing authorization checks on the `cc_whmcs_bridge_add_admin` function, low-level authenticated users such as subscribers can exploit this vulnerability.

Random Banner <= 4.1.4 Admin+ Stored Cross-Site Scripting

Affected Plugin: Random Banner
Plugin Slug: random-banner
Affected Versions: <= 4.1.4
CVE ID: CVE-2022-0210
CVSS Score: 4.8 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:C/C:L/I:L/A:N
Researcher/s: Big Tiger
Fully Patched Version: No patch available, plugin closed for download.
Recommended Remediation: Uninstall Plugin.
Publication Date: 2022-01-14

The Random Banner WordPress plugin is vulnerable to Stored Cross-Site Scripting due to insufficient escaping via the `category` parameter found in the ~/include/models/model.php file which allowed attackers with administrative user access to inject arbitrary web scripts, in versions up to and including 4.1.4. This affects multi-site installations where `unfiltered_html` is disabled for administrators, and sites where `unfiltered_html` is disabled.

XootiX Plugins <= Various Versions Cross-Site Request Forgery to Arbitrary Options Update

Affected Plugins: Login/Signup Popup | Waitlist Woocommerce (Back in stock notifier) | Side Cart Woocommerce (Ajax)
Plugin Slugs: easy-login-woocommerce | waitlist-woocommerce | side-cart-woocommerce
Affected Versions: <= 2.2 | <= 2.5.1 | <= 2.0
CVE ID: CVE-2022-0215
CVSS Score: 8.8 (High)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
Researcher/s: Chloe Chamberland
Fully Patched Version: 2.3 | 2.5.2 | 2.1
Recommended Remediation: Update to the patched versions of each plugin.
Publication Date: 2022-01-13

The Login/Signup Popup, Waitlist Woocommerce (Back in stock notifier), and Side Cart Woocommerce (Ajax) WordPress plugins by XootiX are vulnerable to Cross-Site Request Forgery via the `save_settings` function found in the ~/includes/xoo-framework/admin/class-xoo-admin-settings.php file which makes it possible for attackers to update arbitrary options on a site that can be used to create an administrative user account and grant full privileged access to a compromised site. This affects versions <= 2.2 in Login/Signup Popup, versions <= 2.5.1 in Waitlist Woocommerce (Back in stock notifier), and versions <= 2.0 in Side Cart Woocommerce (Ajax). Read more here.

Crisp Live Chat <= 0.31 Cross-Site Request Forgery to Stored Cross-Site Scripting

Affected Plugin: Crisp Live Chat
Plugin Slug: crisp
Affected Versions: <= 0.31
CVE ID: CVE-2021-43353
CVSS Score: 8.8 (High)
CVSS Vector:CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
Researcher/s: José Aguilera
Fully Patched Version: 0.32
Recommended Remediation: Update to version 0.32, or newer
Publication Date: 2021-12-16

The Crisp Live Chat WordPress plugin is vulnerable to Cross-Site Request Forgery due to missing nonce validation via the `crisp_plugin_settings_page` function found in the ~/crisp.php file, which made it possible for attackers to inject arbitrary web scripts in versions up to, and including 0.31.

WooCommerce myghpay Payment Gateway <= 3.0 Reflected Cross-Site

Affected Plugin: WooCommerce myghpay Payment Gateway
Plugin Slug: woo-myghpay-payment-gateway
Affected Versions: <= 3.0
CVE ID: CVE-2021-39308
CVSS Score: 6.1 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
Researcher/s: p7e4
Fully Patched Version: No patch available, plugin closed for download.
Recommended Remediation: Uninstall Plugin.
Publication Date: 2021-12-14

The WooCommerce myghpay Payment Gateway WordPess plugin is vulnerable to Reflected Cross-Site Scripting via the `clientref` parameter found in the ~/processresponse.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 2.0.8.

True Ranker <= 2.2.2 Directory Traversal/Arbitrary File Read

Affected Plugin: True Ranker
Plugin Slug: seo-local-rank
Affected Versions: <= 2.2.2
CVE ID: CVE-2021-39312
CVSS Score: 7.5 (High)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
Researcher/s: p7e4
Fully Patched Version: 2.2.4
Recommended Remediation: Update to version 2.2.4, or newer.
Publication Date: 2021-12-13

The True Ranker plugin <= 2.2.2 for WordPress allows arbitrary files, including sensitive configuration files such as wp-config.php, to be accessed via the `src` parameter found in the ~/admin/vendor/datatables/examples/resources/examples.php file.

---

duoFAQ – Responsive, Flat, Simple FAQ <= 1.4.8 Reflected Cross-Site Scripting

Affected Plugin: duoFAQ – Responsive, Flat, Simple FAQ
Plugin Slug: duofaq-responsive-flat-simple-faq
Affected Versions: <= 1.4.8
CVE ID: CVE-2021-39319
CVSS Score: 6.1 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
Researcher/s: p7e4
Fully Patched Version: No patch available, plugin closed for download.
Recommended Remediation: Uninstall Plugin.
Publication Date: 2021-12-13

The duoFAQ – Responsive, Flat, Simple FAQ WordPess plugin is vulnerable to Reflected Cross-Site Scripting via the `msg` parameter found in the ~/duogeek/duogeek-panel.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 1.4.8.

H5P CSS Editor <= 1.0 Reflected Cross-Site Scripting

Affected Plugin: H5P CSS Editor
Plugin Slug: h5p-css-editor
Affected Versions: <= 1.0
CVE ID: CVE-2021-39318
CVSS Score: 6.1 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
Researcher/s: p7e4
Fully Patched Version: No patch available, plugin closed for download.
Recommended Remediation: Uninstall Plugin.
Publication Date: 2021-12-13

The H5P CSS Editor WordPress plugin is vulnerable to Reflected Cross-Site Scripting via the `h5p-css-file` parameter found in the ~/h5p-css-editor.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 1.0.

Magic Post Voice <= 1.2 Reflected Cross-Site Scripting

Affected Plugin: Magic Post Voice
Plugin Slug: magic-post-voice
Affected Versions: <= 1.2
CVE ID: CVE-2021-39315
CVSS Score: 6.1 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
Researcher/s: p7e4
Fully Patched Version: No patch available, plugin closed for download.
Recommended Remediation: Uninstall Plugin.
Publication Date: 2021-12-13

The Magic Post Voice WordPress plugin is vulnerable to Reflected Cross-Site Scripting via the `ids` parameter found in the ~/inc/admin/main.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 1.2.

WooCommerce EnvioPack <= 1.2 Reflected Cross-Site Scripting

Affected Plugin: WooCommerce EnvioPack
Plugin Slug: woo-enviopack
Affected Versions: <= 1.2
CVE ID: CVE-2021-39314
CVSS Score: 6.1 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
Researcher/s: p7e4
Fully Patched Version: No patch available, plugin closed for download.
Recommended Remediation: Uninstall Plugin.
Publication Date: 2021-12-13

The WooCommerce EnvioPack WordPress plugin is vulnerable to Reflected Cross-Site Scripting via the `dataid` parameter found in the ~/includes/functions.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 1.2.

Simple Image Gallery <= 1.0.6 Reflected Cross-Site Scripting

Affected Plugin: Simple Image Gallery
Plugin Slug: simple-responsive-image-gallery
Affected Versions: <= 1.0.6
CVE ID: CVE-2021-39313
CVSS Score: 6.1 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
Researcher/s: p7e4
Fully Patched Version: No patch available, plugin closed for download.
Recommended Remediation: Uninstall Plugin.
Publication Date: 2021-12-13

The Simple Image Gallery WordPress plugin is vulnerable to Reflected Cross-Site Scripting via the `msg` parameter found in the ~/simple-image-gallery.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 1.0.6.

---

link-list-manager <= 1.0 Reflected Cross-Site Scripting

Affected Plugin: link-list-manager
Plugin Slug: link-list-manager
Affected Versions: <= 1.0
CVE ID: CVE-2021-39311
CVSS Score: 6.1 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
Researcher/s: p7e4
Fully Patched Version: No patch available, plugin closed for download.
Recommended Remediation: Uninstall Plugin.
Publication Date: 2021-12-13

The link-list-manager WordPress plugin is vulnerable to Reflected Cross-Site Scripting via the `category` parameter found in the ~/llm.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 1.0.

Real WYSIWYG <= 0.0.2 Reflected Cross-Site Scripting

Plugin Slug: real-wysiwyg
Affected Versions: <= 0.0.2
CVE ID: CVE-2021-39310
CVSS Score: 6.1 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
Researcher/s: p7e4
Fully Patched Version: No patch available, plugin closed for download.
Recommended Remediation: Uninstall Plugin.
Publication Date: 2021-12-13

The Real WYSIWYG WordPress plugin is vulnerable to Reflected Cross-Site Scripting due to the use of PHP_SELF in the ~/real-wysiwyg.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 0.0.2.

Parsian Bank Gateway for Woocommerce <= 1.0 Reflected Cross-Site Scripting

Affected Plugin: Parsian Bank Gateway for Woocommerce
Plugin Slug: parsian-bank-gateway-for-woocommerce
Affected Versions: <= 1.0
CVE ID: CVE-2021-39309
CVSS Score: 6.1 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
Researcher/s: p7e4
Fully Patched Version: No patch available, plugin closed for download.
Recommended Remediation: Uninstall Plugin.
Publication Date: 2021-12-13

The Parsian Bank Gateway for Woocommerce WordPress plugin is vulnerable to Reflected Cross-Site Scripting via the `demo` parameter found in the ~/vendor/dpsoft/parsian-payment/sample/rollback-payment.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 1.0.

.htaccess Redirect <= 0.3.1 Reflected Cross-Site Scripting

Affected Plugin: .htaccess Redirect
Plugin Slug: htaccess-redirect
Affected Versions: <= 0.3.1
CVE ID: CVE-2021-38361
CVSS Score: 6.1 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
Researcher/s: p7e4
Fully Patched Version: No patch available, plugin closed for download.
Recommended Remediation: Uninstall Plugin.
Publication Date: 2021-12-13

The .htaccess Redirect WordPress plugin is vulnerable to Reflected Cross-Site Scripting via the `link` parameter found in the ~/htaccess-redirect.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 0.3.1.

RegistrationMagic <= 5.0.1.7 Authentication Bypass

Affected Plugin: RegistrationMagic
Plugin Slug: custom-registration-form-builder-with-submission-manager
Affected Versions: <= 5.0.1.7
CVE ID: CVE-2021-4073
CVSS Score: 9.8 (Critical)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Researcher/s: Marco Wotschka, Chloe Chamberland, and AyeCode Ltd*
Fully Patched Version: 5.0.1.8
Recommended Remediation: Update to version 5.0.1.8, or newer.
Publication Date: 2021-12-08

The RegistrationMagic WordPress plugin made it possible for unauthenticated users to log in as any site user, including administrators, if they knew a valid username on the site due to missing identity validation in the social login function `social_login_using_email()` of the plugin. This affects versions equal to, and less than, 5.0.1.7.

Fathom Analytics <= 3.0.4 Authenticated Stored Cross-Site Scripting

Affected Plugin: Fathom Analytics
Plugin Slug: fathom-analytics
Affected Versions: <= 3.0.4
CVE ID: CVE-2021-41836
CVSS Score: 4.8 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:C/C:L/I:L/A:N
Researcher/s: José Aguilera
Fully Patched Version: 3.0.5
Recommended Remediation: Update to version 3.0.5, or newer.
Publication Date: 2021-12-08

The Fathom Analytics WordPress plugin is vulnerable to Stored Cross-Site Scripting due to insufficient input validation and escaping via the `fathom_site_id` parameter found in the ~/fathom-analytics.php file which allowed attackers with administrative user access to inject arbitrary web scripts, in versions up to and including 3.0.4. This affects multi-site installations where `unfiltered_html` is disabled for administrators, and sites where `unfiltered_html` is disabled.

Variation Swatches for WooCommerce <= 2.1.1 Authenticated Stored Cross-Site Scripting

Affected Plugin: Variation Swatches for WooCommerce
Plugin Slug: variation-swatches-for-woocommerce
Affected Versions: <= 3.0.4
CVE ID: CVE-2021-42367
CVSS Score: 6.1 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
Researcher/s: Chloe Chamberland
Fully Patched Version: 2.1.2
Recommended Remediation: Update to version 2.1.2, or newer.
Publication Date: 2021-12-01

The Variation Swatches for WooCommerce WordPress plugin is vulnerable to Stored Cross-Site Scripting via several parameters found in the ~/includes/class-menu-page.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 2.1.1. Due to missing authorization checks on the `tawcvs_save_settings` function, low-level authenticated users such as subscribers can exploit this vulnerability. Read more here.

Stetic <= 1.0.6 Cross-Site Request Forgery to Stored Cross-Site Scripting

Affected Plugin: Stetic
Plugin Slug: stetic
Affected Versions: <= 1.0.6
CVE ID: CVE-2021-42364
CVSS Score: 8.8 (High)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
Original Researcher/s: Naoki Ogawa, Cryptography Laboratory in Tokyo Denki University
Fully Patched Version: No patch available, plugin closed for download.
Recommended Remediation: Uninstall Plugin.
Publication Date: 2021-11-29

The Stetic WordPress plugin is vulnerable to Cross-Site Request Forgery due to missing nonce validation via the `stats_page` function found in the ~/stetic.php file, which made it possible for attackers to inject arbitrary web scripts in versions up to, and including 1.0.6.

Contact Form With Captcha <= 1.6.2 Cross-Site Request Forgery to Reflected Cross-Site Scripting

Affected Plugin: Contact Form With Captcha
Plugin Slug: contact-form-with-captcha
Affected Versions: <= 1.6.2
CVE ID: CVE-2021-42358

CVSS Score: 8.8 (High)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Publication Date: 2021-11-29

The Contact Form With Captcha WordPress plugin is vulnerable to Cross-Site Request Forgery due to missing nonce validation in the ~/cfwc-form.php file during contact form submission, which made it possible for attackers to inject arbitrary web scripts in versions up to, and including 1.6.2.

Asgaros Forums <= 1.15.13 Authenticated Stored XSS

Affected Plugin: Asgaros Forums
Plugin Slug: asgaros-forum
Affected Versions: <= 1.15.13
CVE ID: CVE-2021-42365
CVSS Score: 4.8 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:C/C:L/I:L/A:N
Researcher/s: Mohammed Aadhil Ashfaq
Fully Patched Version: 1.15.14
Recommended Remediation: Update to version 1.15.14, or newer.
Publication Date: 2021-11-29

The Asgaros Forums WordPress plugin is vulnerable to Stored Cross-Site Scripting due to insufficient escaping via the `name` parameter found in the ~/admin/tables/admin-structure-table.php file which allowed attackers with administrative user access to inject arbitrary web scripts, in versions up to and including 1.15.13. This affects multi-site installations where `unfiltered_html` is disabled for administrators, and sites where `unfiltered_html` is disabled.

Easy Registration Forms <= 2.1.1 Cross-Site Request Forgery to Stored Cross-Site Scripting

Affected Plugin: Easy Registration Forms
Plugin Slug: easy-registration-forms
Affected Versions: <= 2.1.1
CVE ID: CVE-2021-39353
CVSS Score: 8.8 (High)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
Original Researcher/s: Thinkland Security Team
Fully Patched Version: No patch available, plugin closed for download.
Recommended Remediation: Uninstall Plugin.
Publication Date: 2021-11-18

The Easy Registration Forms WordPress plugin is vulnerable to Cross-Site Request Forgery due to missing nonce validation via the `ajax_add_form` function found in the ~/includes/class-form.php file which made it possible for attackers to inject arbitrary web scripts in versions up to, and including 2.1.1.

Preview E-Mails for WooCommerce <= 1.6.8 Reflected Cross-Site Scripting

Affected Plugin: Preview E-Mails for WooCommerce
Plugin Slug: woo-preview-emails
Affected Versions: <= 1.6.8
CVE ID: CVE-2021-42363
CVSS Score: 6.1 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
Original Researcher/s: Chloe Chamberland
Fully Patched Version: 2.0.0
Recommended Remediation: Update to version 2.0.0, or newer.
Publication Date: 2021-11-17

The Preview E-Mails for WooCommerce WordPress plugin is vulnerable to Reflected Cross-Site Scripting via the `search_order` parameter found in the ~/views/form.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 1.6.8. Read more here.

WordPress Popular Posts <= 5.3.2 Authenticated Arbitrary File Upload

Affected Plugin: WordPress Popular Posts
Plugin Slug: wordpress-popular-posts
Affected Versions: <= 5.3.2
CVE ID: CVE-2021-42362
CVSS Score: 8.8 (High)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
Original Researcher/s: Jerome Bruandet, NinTechNet
CVE Requester & Exploit Author: Simone Cristofaro
Fully Patched Version: 5.3.3
Recommended Remediation: Update to version 5.3.3, or newer.
Publication Date: 2021-11-12

The WordPress Popular Posts WordPress plugin is vulnerable to arbitrary file uploads due to insufficient input file type validation found in the ~/src/Image.php file which makes it possible for attackers with contributor level access and above to upload malicious files that can be used to obtain remote code execution, in versions up to and including 5.3.2. Read more here.

Starter Templates — Elementor, Gutenberg & Beaver Builder Templates <= 2.7.0 Authenticated Block Import to Stored XSS

Affected Plugin: Starter Templates — Elementor, Gutenberg & Beaver Builder Templates
Plugin Slug: astra-sites
Affected Versions: <= 2.7.0
CVE ID: CVE-2021-42360
CVSS Score: 7.6 (High)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:H/A:L
Researcher/s: Ramuel Gall
Fully Patched Version: 2.7.1
Recommended Remediation: Update to version 2.7.1, or newer.
Publication Date: 2021-11-12

On sites that also had Elementor installed, it was possible for users with the `edit_posts` capability, which includes Contributor-level users, to import blocks onto any page using the `astra-page-elementor-batch-process` AJAX action. An attacker could craft and host a block containing malicious JavaScript on a server they controlled, and then use it to overwrite any post or page by sending an AJAX request with the action set to `astra-page-elementor-batch-process` and the url parameter pointed to their remotely-hosted malicious block, as well as an id parameter containing the post or page to overwrite.

Any post or page that had been built with Elementor, including published pages, could be overwritten by the imported block, and the malicious JavaScript in the imported block would then be executed in the browser of any visitors to that page. Read more here.

Contact Form Email <= 1.3.24 Authenticated Stored Cross-Site Scripting

Affected Plugin: Contact Form Email
Plugin Slug: contact-form-to-email
Affected Versions: <= 1.3.24
CVE ID: CVE-2021-42361
CVSS Score: 4.8 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:C/C:L/I:L/A:N
Researcher/s: Mohammed Aadhil Ashfaq
Fully Patched Version: 1.3.25
Recommended Remediation: Update to version 1.3.25, or newer.
Publication Date: 2021-11-11

The Contact Form Email WordPress plugin is vulnerable to Stored Cross-Site Scripting due to insufficient input validation and escaping via the `name` parameter found in the ~/trunk/cp-admin-int-list.inc.php file which allowed attackers with administrative user access to inject arbitrary web scripts, in versions up to and including 1.3.24. This only affects multi-site installations where `unfiltered_html` is disabled for administrators, and sites where `unfiltered_html` is disabled.

WP DSGVO Tools (GDPR) <= 3.1.23 Unauthenticated Arbitrary Post Deletion

Affected Plugin: WP DSGVO Tools (GDPR)
Plugin Slug: shapepress-dsgvo

Affected Versions: <= 3.1.23
CVE ID: CVE-2021-42359

Fully Patched Version: 3.1.24
Recommended Remediation: Update to version 3.1.24, or newer.
Publication Date: 2021-11-02

WP DSGVO Tools (GDPR) <= 3.1.23 had an AJAX action, 'admin-dismiss-unsubscribe', which lacked a capability check and a nonce check and was available to unauthenticated users, and did not check the post type when deleting unsubscription requests. As such, it was possible for an attacker to permanently delete an arbitrary post or page on the site by sending an AJAX request with the "action" parameter set to "admin-dismiss-unsubscribe" and the "id" parameter set to the post to be deleted. Sending such a request would move the post to the trash, and repeating the request would permanently delete the post in question.

Google Maps Easy <= 1.9.33 Authenticated Stored Cross-Site Scripting

Affected Plugin: Google Maps Easy
Plugin Slug: google-maps-easy
Affected Versions: <= 1.9.33
CVE ID: CVE-2021-39346
CVSS Score: 5.5 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:L/I:L/A:N
Researcher/s: Thinkland Security Team
Fully Patched Version: 1.10.1
Recommended Remediation: Update to version 1.10.1, or newer.
Publication Date: 2021-11-01

The Google Maps Easy WordPress plugin is vulnerable to Stored Cross-Site Scripting due to insufficient input validation and sanitization via several parameters found in the ~/modules/marker_groups/views/tpl/mgrEditMarkerGroup.php file which allowed attackers with administrative user access to inject arbitrary web scripts, in versions up to and including 1.9.33. This affects multi-site installations where `unfiltered_html` is disabled for administrators, and sites where `unfiltered_html` is disabled.

NextScripts: Social Networks Auto-Poster <= 4.3.20 Reflected Cross-Site Scripting

Affected Plugin: NextScripts: Social Networks Auto-Poster
Plugin Slug: social-networks-auto-poster-facebook-twitter-g
Affected Versions: <= 4.3.20
CVE ID: CVE-2021-38356
CVSS Score: 8.1 (High)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:H
Researcher/s: Ramuel Gall
Fully Patched Version: 4.3.21
Recommended Remediation: Update to version 4.3.21, or newer.
Publication Date: 2021-10-28

The NextScripts: Social Networks Auto-Poster <= 4.3.20 WordPress plugin is vulnerable to Reflected Cross-Site Scripting via the $_REQUEST['page'] parameter which is echoed out on inc/nxs_class_snap.php by supplying the appropriate value 'nxssnap-post' to load the page in $_GET['page'] along with malicious JavaScript in $_POST['page']. Read more here.

OptinMonster <= 2.6.4 Unprotected REST-API Endpoints

Affected Plugin: OptinMonster
Plugin Slug: optinmonster
Affected Versions: <= 2.6.4
CVE ID: CVE-2021-39341
CVSS Score: 7.2 (High)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:L/A:N
Researcher/s: Chloe Chamberland
Fully Patched Version: 2.6.5
Recommended Remediation: Update to version 2.6.5, or newer.
Publication Date: 2021-10-27

The OptinMonster WordPress plugin is vulnerable to sensitive information disclosure and unauthorized setting updates due to insufficient authorization validation via the `logged_in_or_has_api_key` function in the ~/OMAPI/RestApi.php file that can used to exploit inject malicious web scripts on sites with the plugin installed. This affects versions up to, and including, 2.6.4. Read more here.

Hashthemes Demo Importer <= 1.1.1 Improper Access Control Allowing Content Deletion

Affected Plugin: Hashthemes Demo Importer
Plugin Slug: hashthemes-demo-importer
Affected Versions: <= 1.1.1
CVE ID: CVE-2021-39333
CVSS Score: 8.1 (High)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:H
Researcher/s: Ramuel Gall
Fully Patched Version: 1.1.2
Recommended Remediation: Update to version 1.1.2, or newer.
Publication Date: 2021-10-26

The Hashthemes Demo Importer Plugin <= 1.1.1 for WordPress contained several AJAX functions which relied on a nonce which was visible to all logged-in users for access control, allowing them to execute a function that truncated nearly all database tables and removed the contents of wp-content/uploads. Read more here.

Notification – Custom Notifications and Alerts for WordPress <= 7.2.4 Authenticated Stored Cross-Site Scripting

Affected Plugin: Notification – Custom Notifications and Alerts for WordPress
Plugin Slug: notification
Affected Versions: <= 7.2.4
CVE ID: CVE-2021-39340
CVSS Score: 4.8 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:C/C:L/I:L/A:N
Researcher/s: Thinkland Security Team
Fully Patched Version: 8.0.0
Recommended Remediation: Update to version 8.0.0, or newer.
Publication Date: 2021-10-25

The Notification WordPress plugin is vulnerable to Stored Cross-Site Scripting due to insufficient input validation and sanitization via several parameters found in the ~/src/classes/Utils/Settings.php file which made it possible for attackers with administrative user access to inject arbitrary web scripts, in versions up to and including 7.2.4. This affects multi-site installations where `unfiltered_html` is disabled for administrators, and sites where `unfiltered_html` is disabled.

Easy Digital Downloads <= 2.11.2 Authenticated Reflected Cross-Site Scripting

Affected Plugin: Easy Digital Downloads
Plugin Slug: easy-digital-downloads
Affected Versions: <= 2.11.2
CVE ID: CVE-2021-39354
CVSS Score: 4.8 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:C/C:L/I:L/A:N
Researcher/s: Thinkland Security Team
Fully Patched Version: 2.11.2.1
Recommended Remediation: Update to version 2.11.2.1, or newer.
Publication Date: 2021-10-21

The Easy Digital Downloads WordPress plugin is vulnerable to Reflected Cross-Site Scripting via the `$start_date` and `$end_date` parameters found in the ~/includes/admin/payments/class-payments-table.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 2.11.2.

Catch Themes Demo Import <= 1.7 Admin+ Arbitrary File Upload

Affected Plugin: Catch Themes Demo Import
Plugin Slug: catch-themes-demo-import
Affected Versions: <= 1.7

CVE ID: CVE-2021-39352
CVSS Score: 9.1 (Critical)

Recommended Remediation: Update to version 1.8, or newer.
Publication Date: 2021-10-21

The Catch Themes Demo Import WordPress plugin is vulnerable to arbitrary file uploads via the import functionality found in the ~/inc/CatchThemesDemoImport.php file, in versions up to and including 1.7, due to insufficient file type validation. This makes it possible for an attacker with administrative privileges to upload malicious files that can be used to achieve remote code execution.

Simple Job Board <= 2.9.4 Authenticated Stored Cross-Site Scripting

Affected Plugin: Simple Job Board
Plugin Slug: simple-job-board
Affected Versions: <= 2.9.4
CVE ID: CVE-2021-39328
CVSS Score: 5.5 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:L/I:L/A:N
Researcher/s: Thinkland Security Team
Fully Patched Version: 2.9.5
Recommended Remediation: Update to version 2.9.5, or newer.
Publication Date: 2021-10-21

The Simple Job Board WordPress plugin is vulnerable to Stored Cross-Site Scripting due to insufficient escaping on the `$job_board_privacy_policy_label` variable echo'd out via the ~/admin/settings/class-simple-job-board-settings-privacy.php file which allowed attackers with administrative user access to inject arbitrary web scripts, in versions up to and including 2.9.4. This affects multi-site installations where `unfiltered_html` is disabled for administrators, and sites where `unfiltered_html` is disabled.

Sassy Social Share 3.3.23 – PHP Object Injection

Affected Plugin: Sassy Social Share
Plugin Slug: sassy-social-share
Affected Versions: 3.3.23
CVE ID: CVE-2021-39321
CVSS Score: 6.3 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L
Researcher/s: Chloe Chamberland
Fully Patched Version: 3.3.24
Recommended Remediation: Update to version 3.3.24, or newer.
Publication Date: 2021-10-20

Version 3.3.23 of the Sassy Social Share WordPress plugin is vulnerable to PHP Object Injection that can be exploited by subscriber-level users via the `wp_ajax_heateor_sss_import_config` AJAX action due to a missing capability check in the `import_config` function found in the ~/admin/class-sassy-social-share-admin.php file along with the implementation of deserialization on user supplied inputs passed through the `config` parameter. Read more here.

Leaky Paywall <= 4.16.5 Authenticated Stored Cross-Site Scripting

Affected Plugin: Leaky Paywall
Plugin Slug: leaky-paywall
Affected Versions: <= 4.16.5
CVE ID: CVE-2021-39357
CVSS Score: 5.5 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:L/I:L/A:N
Researcher/s: Thinkland Security Team
Fully Patched Version: No patch available, plugin closed for download.
Recommended Remediation: Uninstall Plugin.
Publication Date: 2021-10-18

The Leaky Paywall WordPress plugin is vulnerable to Stored Cross-Site Scripting due to insufficient input validation and sanitization via the ~/class.php file which allowed attackers with administrative user access to inject arbitrary web scripts, in versions up to and including 4.16.5. This affects multi-site installations where `unfiltered_html` is disabled for administrators, and sites where `unfiltered_html` is disabled.

Content Staging <= 2.0.1 Authenticated Stored Cross-Site Scripting

Affected Plugin: Content Staging
Plugin Slug: content-staging
Affected Versions: <= 2.0.1
CVE ID: CVE-2021-39356
CVSS Score: 5.5 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:L/I:L/A:N
Researcher/s: Thinkland Security Team
Fully Patched Version: No patch available, plugin closed for download.
Recommended Remediation: Uninstall Plugin.
Publication Date: 2021-10-18

The Content Staging WordPress plugin is vulnerable to Stored Cross-Site Scripting due to insufficient input validation and escaping via several parameters that are echo'd out via the ~/templates/settings.php file which allowed attackers with administrative user access to inject arbitrary web scripts, in versions up to and including 2.0.1. This affects multi-site installations where `unfiltered_html` is disabled for administrators, and sites where `unfiltered_html` is disabled.

LearnPress – WordPress LMS Plugin <= 4.1.3.1 Authenticated Stored Cross-Site Scripting

Affected Plugin: LearnPress – WordPress LMS Plugin
Plugin Slug: learnpress
Affected Versions: <= 4.1.3.1
CVE ID: CVE-2021-39348
CVSS Score: 5.5 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:L/I:L/A:N
Researcher/s: Thinkland Security Team
Fully Patched Version: 4.1.3.2
Recommended Remediation: Update to version 4.1.3.2, or newer.
Publication Date: 2021-10-18

The LearnPress WordPress plugin is vulnerable to Stored Cross-Site Scripting due to insufficient escaping on the $custom_profile parameter found in the ~/inc/admin/views/backend-user-profile.php file which allowed attackers with administrative user access to inject arbitrary web scripts, in versions up to and including 4.1.3.1. This affects multi-site installations where `unfiltered_html` is disabled for administrators, and sites where `unfiltered_html` is disabled. Please note that this is separate issue from CVE-2021-24702.

Indeed Job Importer <= 1.0.5 Authenticated Stored Cross-Site Scripting

Affected Plugin: Indeed Job Importer
Plugin Slug: indeed-job-importer
Affected Versions: <= 1.0.5
CVE ID: CVE-2021-39355
CVSS Score: 5.5 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:L/I:L/A:N
Researcher/s: Thinkland Security Team
Fully Patched Version: No patch available, plugin closed for download.
Recommended Remediation: Uninstall Plugin.
Publication Date: 2021-10-15

The Indeed Job Importer WordPress plugin is vulnerable to Stored Cross-Site Scripting due to insufficient input validation and sanitization via several parameters found in the ~/indeed-job-importer/trunk/indeed-job-importer.php file which allowed attackers with administrative user access to inject arbitrary web scripts, in versions up to and including 1.0.5. This affects multi-site installations where `unfiltered_html` is disabled for administrators, and sites where `unfiltered_html` is disabled.

MPL-Publisher – Self-publish your book & ebook <= 1.30.2 Authenticated Stored Cross-Site Scripting

Affected Plugin: MPL-Publisher
Plugin Slug: mpl-publisher
Affected Versions: <= 1.30.2
CVE ID: CVE-2021-39343
CVSS Score: 5.5 (Medium)

CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:L/I:L/A:N
Researcher/s: Thinkland Security Team

The MPL-Publisher WordPress plugin is vulnerable to Stored Cross-Site Scripting due to insufficient input validation and sanitization via several parameters found in the ~/libs/PublisherController.php file which allowed attackers with administrative user access to inject arbitrary web scripts, in versions up to and including 1.30.2. This affects multi-site installations where `unfiltered_html` is disabled for administrators, and sites where `unfiltered_html` is disabled.

JobBoardWP – Job Board Listings and Submissions <= 1.0.7 Authenticated Stored Cross-Site Scripting

Affected Plugin: JobBoardWP – Job Board Listings and Submissions
Plugin Slug: jobboardwp
Affected Versions: <= 1.0.7
CVE ID: CVE-2021-39329
CVSS Score: 5.5 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:L/I:L/A:N
Researcher/s: Thinkland Security Team
Fully Patched Version: No patch available, plugin closed for download.
Recommended Remediation: Uninstall Plugin.
Publication Date: 2021-10-15

The JobBoardWP WordPress plugin is vulnerable to Stored Cross-Site Scripting due to insufficient input validation and sanitization via several parameters found in the ~/includes/admin/class-metabox.php file which allowed attackers with administrative user access to inject arbitrary web scripts, in versions up to and including 1.0.6. This affects multi-site installations where `unfiltered_html` is disabled for administrators, and sites where `unfiltered_html` is disabled.

Author Bio Box <= 3.3.1 Authenticated Stored Cross-Site Scripting

Affected Plugin: Author Bio Box
Plugin Slug: author-bio-box
Affected Versions: <= 3.3.1
CVE ID: CVE-2021-39349
CVSS Score: 5.5 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:L/I:L/A:N
Researcher/s: Thinkland Security Team
Fully Patched Version: No patch available, plugin closed for download.
Recommended Remediation: Uninstall Plugin.
Publication Date: 2021-10-14

The Author Bio Box WordPress plugin is vulnerable to Stored Cross-Site Scripting due to insufficient input validation and sanitization via several parameters found in the ~/includes/admin/class-author-bio-box-admin.php file which allowed attackers with administrative user access to inject arbitrary web scripts, in versions up to and including 3.3.1. This affects multi-site installations where `unfiltered_html` is disabled for administrators, and sites where `unfiltered_html` is disabled.

HAL <= 2.1.1 Authenticated Stored Cross-Site Scripting

Affected Plugin: HAL
Plugin Slug: hal
Affected Versions: <= 2.1.1
CVE ID: CVE-2021-39345
CVSS Score: 5.5 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:L/I:L/A:N
Researcher/s: Thinkland Security Team
Fully Patched Version: No patch available, plugin closed for download.
Recommended Remediation: Uninstall Plugin.
Publication Date: 2021-10-14

The HAL WordPress plugin is vulnerable to Stored Cross-Site Scripting due to insufficient input validation and sanitization via several parameters found in the ~/wp-hal.php file which allowed attackers with administrative user access to inject arbitrary web scripts, in versions up to and including 2.1.1. This affects multi-site installations where `unfiltered_html` is disabled for administrators, and sites where `unfiltered_html` is disabled.

KJM Admin Notices <= 2.0.1 Authenticated Stored Cross-Site Scripting

Affected Plugin: KJM Admin Notices
Plugin Slug: kjm-admin-notices
Affected Versions: <= 2.0.1
CVE ID: CVE-2021-39344
CVSS Score: 5.5 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:L/I:L/A:N
Researcher/s: Thinkland Security Team
Fully Patched Version: No patch available, plugin closed for download.
Recommended Remediation: Uninstall Plugin.
Publication Date: 2021-10-14

The KJM Admin Notices WordPress plugin is vulnerable to Stored Cross-Site Scripting due to insufficient input validation and sanitization via several parameters found in the ~/admin/class-kjm-admin-notices-admin.php file which allowed attackers with administrative user access to inject arbitrary web scripts, in versions up to and including 2.0.1. This affects multi-site installations where `unfiltered_html` is disabled for administrators, and sites where `unfiltered_html` is disabled.

MyBB Cross-Poster <= 1.0 Authenticated Stored Cross-Site Scripting

Affected Plugin: MyBB Cross-Poster
Plugin Slug: mybb-cross-poster
Affected Versions: <= 1.0
CVE ID: CVE-2021-39338
CVSS Score: 5.5 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:L/I:L/A:N
Researcher/s: Thinkland Security Team
Fully Patched Version: No patch available, plugin closed for download.
Recommended Remediation: Uninstall Plugin.
Publication Date: 2021-10-14

The MyBB Cross-Poster WordPress plugin is vulnerable to Stored Cross-Site Scripting due to insufficient input validation and sanitization via several parameters found in the ~/classes/MyBBXPSettings.php file which allowed attackers with administrative user access to inject arbitrary web scripts, in versions up to and including 1.0. This affects multi-site installations where `unfiltered_html` is disabled for administrators, and sites where `unfiltered_html` is disabled.

---

job-portal <= 0.0.1 Authenticated Stored Cross-Site Scripting

Affected Plugin: job-portal
Plugin Slug: job-portal
Affected Versions: <= 0.0.1
CVE ID: CVE-2021-39337
CVSS Score: 5.5 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:L/I:L/A:N
Researcher/s: Thinkland Security Team
Fully Patched Version: No patch available, plugin closed for download.
Recommended Remediation: Uninstall Plugin.
Publication Date: 2021-10-14

The job-portal WordPress plugin is vulnerable to Stored Cross-Site Scripting due to insufficient input validation and sanitization via several parameters found in the ~/admin/jobs_function.php file which allowed attackers with administrative user access to inject arbitrary web scripts, in versions up to and including 0.0.1. This affects multi-site installations where `unfiltered_html` is disabled for administrators, and sites where `unfiltered_html` is disabled.

Job Manager <= 0.7.25 Authenticated Stored Cross-Site Scripting

Affected Plugin: Job Manager
Plugin Slug: job-manager
Affected Versions: <= 0.7.25
CVE ID: CVE-2021-39336
CVSS Score: 5.5 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:L/I:L/A:N
Researcher/s: Thinkland Security Team
Fully Patched Version: No patch available, plugin closed for download.

Recommended Remediation: Uninstall Plugin.
Publication Date: 2021-10-14

scripts, in versions up to and including 0.7.25. This affects multi-site installations where `unfiltered_html` is disabled for administrators, and sites where `unfiltered_html` is disabled.

WpGenius Job Listing <= 1.0.2 Authenticated Stored Cross-Site Scripting

Affected Plugin: WpGenius Job Listing
Plugin Slug: wpgenious-job-listing
Affected Versions: <= 1.0
CVE ID: CVE-2021-39335
CVSS Score: 5.5 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:L/I:L/A:N
Researcher/s: Thinkland Security Team
Fully Patched Version: No patch available, plugin closed for download.
Recommended Remediation: Uninstall Plugin.
Publication Date: 2021-10-14

The WpGenius Job Listing WordPress plugin is vulnerable to Stored Cross-Site Scripting due to insufficient input validation and sanitization via several parameters found in the ~/src/admin/class/class-wpgenious-job-listing-options.php file which allowed attackers with administrative user access to inject arbitrary web scripts, in versions up to and including 1.0.2. This affects multi-site installations where `unfiltered_html` is disabled for administrators, and sites where `unfiltered_html` is disabled.

Job Board Vanila Plugin <= 1.0 Authenticated Stored Cross-Site Scripting

Affected Plugin: Job Board Vanila Plugin
Plugin Slug: job-board-vanilla
Affected Versions: <= 1.0
CVE ID: CVE-2021-39334
CVSS Score: 5.5 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:L/I:L/A:N
Researcher/s: Thinkland Security Team
Fully Patched Version: No patch available, plugin closed for download.
Recommended Remediation: Uninstall Plugin.
Publication Date: 2021-10-14

The Job Board Vanila WordPress plugin is vulnerable to Stored Cross-Site Scripting due to insufficient input validation and sanitization via the `psjb_exp_in` and the `psjb_curr_in` parameters found in the ~/job-settings.php file which allowed attackers with administrative user access to inject arbitrary web scripts, in versions up to and including 1.4.5. This affects multi-site installations where `unfiltered_html` is disabled for administrators, and sites where `unfiltered_html` is disabled.

Business Manager – WordPress ERP, HR, CRM, and Project Management Plugin <= 1.4.5 Authenticated Stored Cross-Site Scripting

Affected Plugin: Business Manager
Plugin Slug: business-manager
Affected Versions: <= 1.4.5
CVE ID: CVE-2021-39332
CVSS Score: 5.5 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:L/I:L/A:N
Researcher/s: Thinkland Security Team
Fully Patched Version: No patch available, plugin closed for download.
Recommended Remediation: Uninstall Plugin.
Publication Date: 2021-10-14

The Business Manager WordPress plugin is vulnerable to Stored Cross-Site Scripting due to insufficient input validation and sanitization found throughout the plugin which allowed attackers with administrative user access to inject arbitrary web scripts, in versions up to and including 1.4.5. This affects multi-site installations where `unfiltered_html` is disabled for administrators, and sites where `unfiltered_html` is disabled.

Brizy – Page Builder <= 2.3.11 Authenticated File Upload and Path Traversal

Affected Plugin: Brizy – Page Builder
Plugin Slug: brizy
Affected Versions: <= 2.3.11
CVE ID: CVE-2021-38346
CVSS Score: 8.8 (High)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
Researcher/s: Ramuel Gall
Fully Patched Version: 2.3.12
Recommended Remediation: Update to version 2.3.12, or newer.
Publication Date: 2021-10-13

The Brizy Page Builder plugin <= 2.3.11 for WordPress allowed authenticated users to upload executable files to a location of their choice using the `brizy_create_block_screenshot` AJAX action. The file would be named using the id parameter, which could be prepended with "../" to perform directory traversal, and the file contents were populated via the ibsf parameter, which would be base64-decoded and written to the file. While the plugin added a .jpg extension to all uploaded filenames, a double extension attack was still possible, e.g. a file named shell.php would be saved as shell.php.jpg, and would be executable on a number of common configurations. Read more here.

Brizy – Page Builder <= 2.3.11 Authenticated Stored Cross-Site Scripting

Affected Plugin: Brizy – Page Builder
Plugin Slug: brizy
Affected Versions: <= 2.3.11
CVE ID: CVE-2021-38344
CVSS Score: 6.4 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:N
Researcher/s: Ramuel Gall
Fully Patched Version: 2.3.12
Recommended Remediation: Update to version 2.3.12, or newer.
Publication Date: 2021-10-13

The Brizy Page Builder plugin <= 2.3.11 for WordPress was vulnerable to stored XSS by lower-privileged users such as a subscribers. It was possible to add malicious JavaScript to a page by modifying the request sent to update the page via the `brizy_update_item` AJAX action and adding JavaScript to the data parameter, which would be executed in the session of any visitor viewing or previewing the post or page. Read more here.

Brizy – Page Builder <= 1.0.125 and 1.0.127 – 2.3.11 Incorrect Authorization Checks Allowing Post Modification

Affected Plugin: Brizy – Page Builder
Plugin Slug: brizy
Affected Versions: <= 1.0.125 and 1.0.127 – 2.3.11
CVE ID: CVE-2021-38345
CVSS Score: 7.1 (High)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:L
Researcher/s: Ramuel Gall
Fully Patched Version: 2.3.12
Recommended Remediation: Update to version 2.3.12, or newer.
Publication Date: 2021-10-13

The Brizy Page Builder plugin <= 2.3.11 for WordPress used an incorrect authorization check that allowed any logged-in user accessing any endpoint in the wp-admin directory to modify the content of any existing post or page created with the Brizy editor. An identical issue was found by another researcher in Brizy <= 1.0.125 and fixed in version 1.0.126, but the vulnerability was reintroduced in version 1.0.127. Read more here.

Formidable Form Builder – Contact Form, Survey & Quiz Forms Plugin for WordPress <= 5.0.06 Authenticated Stored Cross-Site Scripting

Affected Plugin: Formidable Form Builder – Contact Form, Survey & Quiz Forms Plugin for WordPress
Plugin Slug: formidable
Affected Versions: <= 5.0.06
CVE ID: CVE-2021-39330

CVSS Score: 5.5 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:L/I:L/A:N

Publication Date: 2021-10-13

The Formidable Form Builder WordPress plugin is vulnerable to Stored Cross-Site Scripting due to insufficient input validation and sanitization found in the ~/classes/helpers/FrmAppHelper.php file which allowed attackers with administrative user access to inject arbitrary web scripts, in versions up to and including 5.0.06. This only affects multi-site installations where `unfiltered_html` is disabled for administrators, and sites where `unfiltered_html` is disabled.

Access Demo Importer <= 1.0.6 – Authenticated Arbitrary File Upload

Affected Plugin: Access Demo Importer
Plugin Slug: access-demo-importer
Affected Versions: <= 1.0.6
CVE ID: CVE-2021-39317
CVSS Score: 8.8 (High)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
Researcher/s: Chloe Chamberland
Fully Patched Version: 1.0.7
Recommended Remediation: Update to version 1.0.7, or newer.
Publication Date: 2021-10-06

Versions up to, and including, 1.0.6, of the Access Demo Importer WordPress plugin are vulnerable to arbitrary file uploads via the `plugin_offline_installer` AJAX action due to a missing capability check in the `plugin_offline_installer_callback` function found in the ~/inc/demo-functions.php. Read more here.

WP Bannerize 2.0.0 – 4.0.2 – Authenticated SQL Injection

Affected Plugin: WP Bannerize
Plugin Slug: wp-bannerize
Affected Versions: 2.0.0 – 4.0.2
CVE ID: CVE-2021-39351
CVSS Score: 7.7 (High)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N
Researcher/s: Margaux DABERT from Intrinsec
Fully Patched Version: Unpatched.
Recommended Remediation: Uninstall Plugin.
Publication Date: 2021-10-05

The WP Bannerize WordPress plugin is vulnerable to authenticated SQL injection via the `id` parameter found in the ~/Classes/wpBannerizeAdmin.php file which allows attackers to exfiltrate sensitive information from vulnerable sites. This issue affects versions 2.0.0 – 4.0.2.

FV Flowplayer Video Player <= 7.5.0.727 – 7.5.2.727 Reflected Cross-Site Scripting

Affected Plugin: FV Flowplayer Video Player
Plugin Slug: fv-wordpress-flowplayer
Affected Versions: 7.5.0.727 – 7.5.2.727
CVE ID: CVE-2021-39350
CVSS Score: 6.1 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
Researcher/s: Margaux DABERT from Intrinsec & Erwan from WPScan*
Fully Patched Version: 7.5.3.727
Recommended Remediation: Update to version 7.5.3.727, or newer.
Publication Date: 2021-10-05

The FV Flowplayer Video Player WordPress plugin is vulnerable to Reflected Cross-Site Scripting via the `player_id` parameter found in the ~/view/stats.php file which allows attackers to inject arbitrary web scripts, in versions 7.5.0.727 – 7.5.2.727.

*Both researchers discovered this vulnerability independently around the same time and both disclosed to the vendor independently.

Stripe for WooCommerce 3.0.0 – 3.3.9 Missing Authorization Controls to Financial Account Hijacking

Affected Plugin: Stripe for WooCommerce
Plugin Slug: woo-stripe-payment
Affected Versions: 3.0.0 – 3.3.9
CVE ID: CVE-2021-39347
CVSS Score: 4.3 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N
Researcher/s: Margaux DABERT from Intrinsec
Fully Patched Version: 3.3.10
Recommended Remediation: Update to version 3.3.10, or newer.
Publication Date: 2021-10-01

The Stripe for WooCommerce WordPress plugin is missing a capability check on the `save()` function found in the ~/includes/admin/class-wc-stripe-admin-user-edit.php file that makes it possible for attackers to configure their account to use other site users unique STRIPE identifier and make purchases with their payment accounts. This affects versions 3.0.0 – 3.3.9.

Credova_Financial <= 1.4.8 Sensitive Information Disclosure

Affected Plugin: Credova_Financial
Plugin Slug: credova-financial
Affected Versions: <= 1.4.8
CVE ID: CVE-2021-39342
CVSS Score: 5.3 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
Researcher/s: Marvin Santos
Fully Patched Version: 1.4.9
Recommended Remediation: Update to version 1.4.9, or newer.
Publication Date: 2021-09-29

The Credova_Financial WordPress plugin discloses a site's associated Credova API account username and password in plaintext via an AJAX action whenever a site user goes to checkout on a page that has the Credova Financing option enabled. This affects versions up to, and including, 1.4.8.

Countdown and CountUp, WooCommerce Sales Timers <= 1.5.7 Cross-Site Request Forgery to Stored Cross-Site Scripting

Affected Plugin: Countdown and CountUp, WooCommerce Sales Timers
Plugin Slug: countdown-wpdevart-extended
Affected Versions: <= 1.5.7
CVE ID: CVE-2021-34636
CVSS Score: 8.8 (High)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
Researcher/s: Xu-Liang Liao
Fully Patched Version: 1.5.8
Recommended Remediation: Update to version 1.5.8, or newer.
Publication Date: 2021-09-27

The Countdown and CountUp, WooCommerce Sales Timers WordPress plugin is vulnerable to Cross-Site Request Forgery via the `save_theme` function found in the ~/includes/admin/coundown_theme_page.php file due to a missing nonce check which allows attackers to inject arbitrary web scripts, in versions up to and including 1.5.7.

Ninja Forms <= 3.5.7 Unprotected REST-API to Email Injection

Affected Plugin: Ninja Forms
Plugin Slug: ninja-forms
Affected Versions: <= 3.5.7
CVE ID: CVE-2021-34648
CVSS Score: 6.5 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:N
Researcher/s: Chloe Chamberland
Fully Patched Version: 3.5.8

Recommended Remediation: Update to version 3.5.8, or newer.
Publication Date: 2021-09-22

emails from the affected server via the /ninja-forms-submissions/email-action REST API which can be used to socially engineer victims. Read more here.

Ninja Forms <= 3.5.7 Unprotected REST-API to Sensitive Information Disclosure

Affected Plugin: Ninja Forms
Plugin Slug: ninja-forms
Affected Versions: <= 3.5.7
CVE ID: CVE-2021-34647
CVSS Score: 6.5 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N
Researcher/s: Chloe Chamberland
Fully Patched Version: 3.5.8
Recommended Remediation: Update to version 3.5.8, or newer.
Publication Date: 2021-09-22

The Ninja Forms WordPress plugin is vulnerable to sensitive information disclosure via the `bulk_export_submissions` function found in the ~/includes/Routes/Submissions.php file, in versions up to and including 3.5.7. This allows authenticated attackers to export all Ninja Forms submissions data via the /ninja-forms-submissions/export REST API which can include personally identifiable information. Read more here.

Telefication <= 1.8.0 Open Relay and Server-Side Request Forgery

Affected Plugin: Telefication
Plugin Slug: telefication
Affected Versions: <= 1.8.0
CVE ID: CVE-2021-39339
CVSS Score: 5.8 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:L
Researcher/s: Marco Wotschka & Charles Strader Sweethill
Fully Patched Version: No patch available, plugin closed for download.
Recommended Remediation: Uninstall Plugin.
Publication Date: 2021-09-21

The Telefication WordPress plugin is vulnerable to Open Proxy and Server-Side Request Forgery via the ~/bypass.php file due to a user-supplied URL request value that gets called by a curl requests. This affects versions up to, and including, 1.8.0.

OptinMonster <= 2.6.0 Reflected Cross-Site Scripting

Affected Plugin: OptinMonster
Plugin Slug: optinmonster
Affected Versions: <= 2.6.0
CVE ID: CVE-2021-39325
CVSS Score: 6.1 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
Researcher/s: Mariia Aleksandrova
Fully Patched Version: 2.6.1
Recommended Remediation: Update to version 2.6.1, or newer.
Publication Date: 2021-09-20

The OptinMonster WordPress plugin is vulnerable to Reflected Cross-Site Scripting due to insufficient input validation in the `load_previews` function found in the ~/OMAPI/Output.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 2.6.0.

eID Easy <= 4.6 Reflected Cross-Site Scripting

Affected Plugin: eID Easy
Plugin Slug: smart-id
Affected Versions: <= 4.6
CVE ID: CVE-2021-34650
CVSS Score: 6.1 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
Researcher/s: p7e4
Fully Patched Version: 4.7
Recommended Remediation: Update to version 4.7, or newer.
Publication Date: 2021-09-17

The eID Easy WordPress plugin is vulnerable to Reflected Cross-Site Scripting via the error parameter found in the ~/admin.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 4.6.

BulletProof Security <= 5.1 Sensitive Information Disclosure

Affected Plugin: BulletProof Security
Plugin Slug: bulletproof-security
Affected Versions: <= 5.1
CVE ID: CVE-2021-39327
CVSS Score: 5.3 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
Researcher/s: Vincent Rakotomanga
Fully Patched Version: 5.2
Recommended Remediation: Update to version 5.2, or newer.
Publication Date: 2021-09-16

The BulletProof Security WordPress plugin is vulnerable to sensitive information disclosure due to a file path disclosure in the publicly accessible ~/db_backup_log.txt file which grants attackers the full path of the site, in addition to the path of database backup files. This affects versions up to, and including, 5.1.

wp-publications <= 0.0 Local File Include

Affected Plugin: wp-publications
Plugin Slug: wp-publications
Affected Versions: <= 0.0
CVE ID: CVE-2021-38360
CVSS Score: 8.3 (High)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:L/A:L
Researcher/s: p7e4
Fully Patched Version: No patch available, plugin closed for download.
Recommended Remediation: Uninstall Plugin.
Publication Date: 2021-09-09

The wp-publications WordPress plugin is vulnerable to restrictive local file inclusion via the `Q_FILE` parameter found in the ~/bibtexbrowser.php file which allows attackers to include local zip files and achieve remote code execution, in versions up to and including 0.0.

WordPress InviteBox Plugin for viral Refer-a-Friend Promotions <= 1.4.1 Reflected Cross-Site Scripting

Affected Plugin: WordPress InviteBox Plugin
Plugin Slug: refer-a-friend-widget-for-wp
Affected Versions: <= 1.4.1
CVE ID: CVE-2021-38359
CVSS Score: 6.1 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
Researcher/s: p7e4
Fully Patched Version: No patch available, plugin closed for download.
Recommended Remediation: Uninstall Plugin.
Publication Date: 2021-09-09

The WordPress InviteBox Plugin for viral Refer-a-Friend Promotions WordPress plugin is vulnerable to Reflected Cross-Site Scripting via the `message` parameter found in the ~/admin/admin.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 1.4.1.

MoolaMojo <= 0.7.4.1 Reflected Cross-Site Scripting

Affected Versions: <= 0.7.4.1
CVE ID: CVE-2021-38358
CVSS Score: 6.1 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
Researcher/s: p7e4
Fully Patched Version: No patch available, plugin closed for download.
Recommended Remediation: Uninstall Plugin.
Publication Date: 2021-09-09

The MoolaMojo WordPress plugin is vulnerable to Reflected Cross-Site Scripting via the `classes` parameter found in the ~/views/button-generator.html.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 0.7.4.1.

SMS OVH <= 0.1 Reflected Cross-Site Scripting

Affected Plugin: SMS OVH
Plugin Slug: sms-ovh
Affected Versions: <= 0.1
CVE ID: CVE-2021-38357
CVSS Score: 6.1 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
Researcher/s: p7e4
Fully Patched Version: No patch available, plugin closed for download.
Recommended Remediation: Uninstall Plugin.
Publication Date: 2021-09-09

The SMS OVH WordPress plugin is vulnerable to Reflected Cross-Site Scripting via the `position` parameter found in the ~/sms-ovh-sent.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 0.1.

Bug Library <= 2.0.3 Reflected Cross-Site Scripting

Affected Plugin: Bug Library
Plugin Slug: bug-library
Affected Versions: <= 2.0.3
CVE ID: CVE-2021-38355
CVSS Score: 6.1 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
Researcher/s: p7e4
Fully Patched Version: No patch available, plugin closed for download.
Recommended Remediation: Uninstall Plugin.
Publication Date: 2021-09-09

The Bug Library WordPress plugin is vulnerable to Reflected Cross-Site Scripting via the `successimportcount` parameter found in the ~/bug-library.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 2.0.3.

GNU-Mailman Integration <= 1.0.6 Reflected Cross-Site Scripting

Affected Plugin: GNU-Mailman Integration
Plugin Slug: gnu-mailman-integration
Affected Versions: <= 1.0.6
CVE ID: CVE-2021-38354
CVSS Score: 6.1 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
Researcher/s: p7e4
Fully Patched Version: No patch available, plugin closed for download.
Recommended Remediation: Uninstall Plugin.
Publication Date: 2021-09-09

The GNU-Mailman Integration WordPress plugin is vulnerable to Reflected Cross-Site Scripting via the `gm_error` parameter found in the ~/includes/admin/mailing-lists-page.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 1.0.6.

Dropdown and scrollable Text <= 2.0 Reflected Cross-Site Scripting

Affected Plugin: Dropdown and scrollable Text
Plugin Slug: dropdown-and-scrollable-text
Affected Versions: <= 2.0
CVE ID: CVE-2021-38353
CVSS Score: 6.1 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
Researcher/s: p7e4
Fully Patched Version: No patch available, plugin closed for download.
Recommended Remediation: Uninstall Plugin.
Publication Date: 2021-09-09

The Dropdown and scrollable Text WordPress plugin is vulnerable to Reflected Cross-Site Scripting via the `content` parameter found in the ~/index.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 2.0.

Feedify – Web Push Notifications <= 2.1.8 Reflected Cross-Site Scripting

Affected Plugin: Feedify – Web Push Notifications
Plugin Slug: push-notification-by-feedify
Affected Versions: <= 2.1.8
CVE ID: CVE-2021-38352
CVSS Score: 6.1 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
Researcher/s: p7e4
Fully Patched Version: No patch available, plugin closed for download.
Recommended Remediation: Uninstall Plugin.
Publication Date: 2021-09-09

The Feedify – Web Push Notifications WordPress plugin is vulnerable to Reflected Cross-Site Scripting via the `feedify_msg` parameter found in the ~/includes/base.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 2.1.8.

OSD Subscribe <= 1.2.3 Reflected Cross-Site Scripting

Affected Plugin: OSD Subscribe
Plugin Slug: osd-subscribe
Affected Versions: <= 1.2.3
CVE ID: CVE-2021-38351
CVSS Score: 6.1 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
Researcher/s: p7e4
Fully Patched Version: No patch available, plugin closed for download.
Recommended Remediation: Uninstall Plugin.
Publication Date: 2021-09-09

The OSD Subscribe WordPress plugin is vulnerable to Reflected Cross-Site Scripting via the `osd_subscribe_message` parameter found in the ~/options/osd_subscribe_options_subscribers.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 1.2.3.

---

spideranalyse <= 0.0.1 Reflected Cross-Site Scripting

Affected Plugin: spideranalyse
Plugin Slug: spideranalyse
Affected Versions: <= 0.0.1
CVE ID: CVE-2021-38350
CVSS Score: 6.1 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
Researcher/s: p7e4
Fully Patched Version: No patch available, plugin closed for download.
Recommended Remediation: Uninstall Plugin.
Publication Date: 2021-09-09

The spideranalyse WordPress plugin is vulnerable to Reflected Cross-Site Scripting via the `date` parameter found in the ~/analyse/index.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 0.0.1.

Integration of Moneybird for WooCommerce <= 2.1.1 Reflected Cross-Site

Affected Plugin: Integration of Moneybird for WooCommerce
Plugin Slug: woo-moneybird
Affected Versions: <= 2.1.1
CVE ID: CVE-2021-38349
CVSS Score: 6.1 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
Researcher/s: p7e4
Fully Patched Version: No patch available, plugin closed for download.
Recommended Remediation: Uninstall Plugin.
Publication Date: 2021-09-09

The Integration of Moneybird for WooCommerce WordPress plugin is vulnerable to Reflected Cross-Site Scripting via the `error_description` parameter found in the ~/templates/wcmb-admin.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 2.1.1.

Advance Search <= 1.1.2 Reflected Cross-Site Scripting

Affected Plugin: Advance Search
Plugin Slug: advance-search
Affected Versions: <= 1.1.2
CVE ID: CVE-2021-38348
CVSS Score: 6.1 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
Researcher/s: p7e4
Fully Patched Version: No patch available, plugin closed for download.
Recommended Remediation: Uninstall Plugin.
Publication Date: 2021-09-09

The Advance Search WordPress plugin is vulnerable to Reflected Cross-Site Scripting via the `wpas_id` parameter found in the ~/inc/admin/views/html-advance-search-admin-options.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 1.1.2.

Custom Website Data <= 2.2 Reflected Cross-Site Scripting

Affected Plugin: Custom Website Data
Plugin Slug: simple-custom-website-data
Affected Versions: <= 2.2
CVE ID: CVE-2021-38347
CVSS Score: 6.1 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
Researcher/s: p7e4
Fully Patched Version: No patch available, plugin closed for download.
Recommended Remediation: Uninstall Plugin.
Publication Date: 2021-09-09

The Custom Website Data WordPress plugin is vulnerable to Reflected Cross-Site Scripting via the `id` parameter found in the ~/views/edit.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 2.2.

WooCommerce Payment Gateway Per Category <= 2.0.10 Reflected Cross-Site Scripting

Affected Plugin: WooCommerce Payment Gateway Per Category
Plugin Slug: wc-payment-gateway-per-category
Affected Versions: <= 2.0.10
CVE ID: CVE-2021-38341
CVSS Score: 6.1 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
Researcher/s: p7e4
Fully Patched Version: No patch available, plugin closed for download.
Recommended Remediation: Uninstall Plugin.
Publication Date: 2021-09-09

The WooCommerce Payment Gateway Per Category WordPress plugin is vulnerable to Reflected Cross-Site Scripting due to a reflected `$_SERVER["PHP_SELF"]` value in the ~/includes/plugin_settings.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 2.0.10.

WordPress Simple Shop <= 1.2 Reflected Cross-Site Scripting

Affected Plugin: WordPress Simple Shop
Plugin Slug: webful-simple-grocery-shop
Affected Versions: <= 1.2
CVE ID: CVE-2021-38340
CVSS Score: 6.1 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
Researcher/s: p7e4
Fully Patched Version: No patch available, plugin closed for download.
Recommended Remediation: Uninstall Plugin.
Publication Date: 2021-09-09

The WordPress Simple Shop WordPress plugin is vulnerable to Reflected Cross-Site Scripting via the `update_row` parameter found in the ~/includes/add_product.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 1.2.

Simple Matted Thumbnails <= 1.01 Reflected Cross-Site Scripting

Affected Plugin: Simple Matted Thumbnails
Plugin Slug: simple-matted-thumbnails
Affected Versions: <= 1.01
CVE ID: CVE-2021-38339
CVSS Score: 6.1 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
Researcher/s: p7e4
Fully Patched Version: No patch available, plugin closed for download.
Recommended Remediation: Uninstall Plugin.
Publication Date: 2021-09-09

The Simple Matted Thumbnails WordPress plugin is vulnerable to Reflected Cross-Site Scripting due to a reflected `$_SERVER["PHP_SELF"]` value in the ~/simple-matted-thumbnail.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 1.01.

Border Loading Bar <= 1.0.1 Reflected Cross-Site Scripting

Affected Plugin: Border Loading Bar
Plugin Slug: border-loading-bar
Affected Versions: <= 1.0.1
CVE ID: CVE-2021-38338
CVSS Score: 6.1 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
Researcher/s: p7e4
Fully Patched Version: No patch available, plugin closed for download.
Recommended Remediation: Uninstall Plugin.
Publication Date: 2021-09-09

The Border Loading Bar WordPress plugin is vulnerable to Reflected Cross-Site Scripting via the `f` and `t` parameter found in the ~/titan-framework/iframe-googlefont-preview.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 1.0.1.

RSVPMaker Excel <= 1.1 Reflected Cross-Site Scripting

Affected Plugin: RSVPMaker Excel
Plugin Slug: rsvpmaker-excel
Affected Versions: <= 1.1
CVE ID: CVE-2021-38337
CVSS Score: 6.1 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
Researcher/s: p7e4
Fully Patched Version: No patch available, plugin closed for download.

Recommended Remediation: Uninstall Plugin.
Publication Date: 2021-09-09

and including 1.1.

Edit Comments XT <= 1.0 Reflected Cross-Site Scripting

Affected Plugin: Edit Comments XT
Plugin Slug: edit-comments-xt
Affected Versions: <= 1.0
CVE ID: CVE-2021-38336
CVSS Score: 6.1 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
Researcher/s: p7e4
Fully Patched Version: No patch available, plugin closed for download.
Recommended Remediation: Uninstall Plugin.
Publication Date: 2021-09-09

The Edit Comments XT WordPress plugin is vulnerable to Reflected Cross-Site Scripting due to a reflected `$_SERVER["PHP_SELF"]` value in the ~/edit-comments-xt.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 1.0.

Wise Agent Capture Forms <= 1.0 Reflected Cross-Site Scripting

Affected Plugin: Wise Agent Capture Forms
Plugin Slug: wiseagentleadform
Affected Versions: <= 1.0
CVE ID: CVE-2021-38335
CVSS Score: 6.1 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
Researcher/s: p7e4
Fully Patched Version: No patch available, plugin closed for download.
Recommended Remediation: Uninstall Plugin.
Publication Date: 2021-09-09

The Wise Agent Capture Forms WordPress plugin is vulnerable to Reflected Cross-Site Scripting due to a reflected `$_SERVER["PHP_SELF"]` value in the ~/WiseAgentCaptureForm.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 1.0.

WP Design Maps & Places <= 1.2 Reflected Cross-Site Scripting

Affected Plugin: WP Design Maps & Places
Plugin Slug: wp-design-maps-places
Affected Versions: <= 1.2
CVE ID: CVE-2021-38334
CVSS Score: 6.1 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
Researcher/s: p7e4
Fully Patched Version: No patch available, plugin closed for download.
Recommended Remediation: Uninstall Plugin.
Publication Date: 2021-09-09

The WP Design Maps & Places WordPress plugin is vulnerable to Reflected Cross-Site Scripting via the `filename` parameter found in the ~/wpdmp-admin.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 1.2.

WP Scrippets <= 1.5.1 Reflected Cross-Site Scripting

Affected Plugin: WP Scrippets
Plugin Slug: wp-scrippets
Affected Versions: <= 1.5.1
CVE ID: CVE-2021-38333
CVSS Score: 6.1 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
Researcher/s: p7e4
Fully Patched Version: No patch available, plugin closed for download.
Recommended Remediation: Uninstall Plugin.
Publication Date: 2021-09-09

The WP Scrippets WordPress plugin is vulnerable to Reflected Cross-Site Scripting due to a reflected `$_SERVER["PHP_SELF"]` value in the ~/wp-scrippets.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 1.5.1.

On Page SEO + Whatsapp Chat Button <= 1.0.1 Reflected Cross-Site Scripting

Affected Plugin: On Page SEO + Whatsapp Chat Button
Plugin Slug: ops-robots-txt
Affected Versions: <= 1.0.1
CVE ID: CVE-2021-38332
CVSS Score: 6.1 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
Researcher/s: p7e4
Fully Patched Version: No patch available, plugin closed for download.
Recommended Remediation: Uninstall Plugin.
Publication Date: 2021-09-09

The On Page SEO + Whatsapp Chat Button Plugin WordPress plugin is vulnerable to Reflected Cross-Site Scripting due to a reflected `$_SERVER["PHP_SELF"]` value in the ~/settings.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 1.0.1.

WP-T-Wap <= 1.13.2 Reflected Cross-Site Scripting

Affected Plugin: WP-T-Wap
Plugin Slug: wp-t-wap
Affected Versions: <= 1.13.2
CVE ID: CVE-2021-38331
CVSS Score: 6.1 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
Researcher/s: p7e4
Fully Patched Version: No patch available, plugin closed for download.
Recommended Remediation: Uninstall Plugin.
Publication Date: 2021-09-09

The WP-T-Wap WordPress plugin is vulnerable to Reflected Cross-Site Scripting via the `posted` parameter found in the ~/wap/writer.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 1.13.2.

Yet Another bol.com Plugin <= 1.4 Reflected Cross-Site Scripting

Affected Plugin: Yet Another bol.com Plugin
Plugin Slug: yabp
Affected Versions: <= 1.4
CVE ID: CVE-2021-38330
CVSS Score: 6.1 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
Researcher/s: p7e4
Fully Patched Version: No patch available, plugin closed for download.
Recommended Remediation: Uninstall Plugin.
Publication Date: 2021-09-09

The Yet Another bol.com Plugin WordPress plugin is vulnerable to Reflected Cross-Site Scripting due to a reflected `$_SERVER["PHP_SELF"]` value in the ~/yabp.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 1.4.

DJ EmailPublish <= 1.7.2 Reflected Cross-Site Scripting

Affected Plugin: DJ EmailPublish
Plugin Slug: dj-email-publish
Affected Versions: <= 1.7.2

CVE ID: CVE-2021-38329
CVSS Score: 6.1 (Medium)

Recommended Remediation: Uninstall Plugin.
Publication Date: 2021-09-09

The DJ EmailPublish WordPress plugin is vulnerable to Reflected Cross-Site Scripting due to a reflected `$_SERVER["PHP_SELF"]` value in the ~/dj-email-publish.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 1.7.2.

Notices <= 6.1 Reflected Cross-Site Scripting

Affected Plugin: Notices
Plugin Slug: notices
Affected Versions: <= 6.1
CVE ID: CVE-2021-38328
CVSS Score: 6.1 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
Researcher/s: p7e4
Fully Patched Version: No patch available, plugin closed for download.
Recommended Remediation: Uninstall Plugin.
Publication Date: 2021-09-09

The Notices WordPress plugin is vulnerable to Reflected Cross-Site Scripting due to a reflected `$_SERVER["PHP_SELF"]` value in the ~/notices.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 6.1.

YouTube Video Inserter <= 1.2.1.0 Reflected Cross-Site Scripting

Affected Plugin: YouTube Video Inserter
Plugin Slug: youtube-video-inserter
Affected Versions: <= 1.2.1.0
CVE ID: CVE-2021-38327
CVSS Score: 6.1 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
Researcher/s: p7e4
Fully Patched Version: No patch available, plugin closed for download.
Recommended Remediation: Uninstall Plugin.
Publication Date: 2021-09-09

The YouTube Video Inserter WordPress plugin is vulnerable to Reflected Cross-Site Scripting due to a reflected `$_SERVER["PHP_SELF"]` value in the ~/adminUI/settings.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 1.2.1.0.

Post Title Counter <= 1.1 Reflected Cross-Site Scripting

Affected Plugin: Post Title Counter
Plugin Slug: post-title-counter
Affected Versions: <= 1.1
CVE ID: CVE-2021-38326
CVSS Score: 6.1 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
Researcher/s: p7e4
Fully Patched Version: No patch available, plugin closed for download.
Recommended Remediation: Uninstall Plugin.
Publication Date: 2021-09-09

The Post Title Counter WordPress plugin is vulnerable to Reflected Cross-Site Scripting via the `notice` parameter found in the ~/post-title-counter.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 1.1.

User Activation Email <= 1.3.0 Reflected Cross-Site Scripting

Affected Plugin: User Activation Email
Plugin Slug: user-activation-email
Affected Versions: <= 1.3.0
CVE ID: CVE-2021-38325
CVSS Score: 6.1 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
Researcher/s: p7e4
Fully Patched Version: No patch available, plugin closed for download.
Recommended Remediation: Uninstall Plugin.
Publication Date: 2021-09-08

The User Activation Email WordPress plugin is vulnerable to Reflected Cross-Site Scripting via the `use-key` parameter found in the ~/user-activation-email.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 1.3.0.

SP Rental Manager <= 1.5.3 Unauthenticated SQL Injection

Affected Plugin: SP Rental Manager
Plugin Slug: sp-rental-manager
Affected Versions: <= 1.5.3
CVE ID: CVE-2021-38324
CVSS Score: 8.2 (High)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:L
Researcher/s: p7e4
Fully Patched Version: No patch available, plugin closed for download.
Recommended Remediation: Uninstall Plugin.
Publication Date: 2021-09-08

The SP Rental Manager WordPress plugin is vulnerable to SQL Injection via the `orderby` parameter found in the ~/user/shortcodes.php file which allows attackers to retrieve information contained in a site's database, in versions up to and including 1.5.3.

RentPress <= 6.6.4 Reflected Cross-Site Scripting

Affected Plugin: RentPress
Plugin Slug: rentpress
Affected Versions: <= 6.6.4
CVE ID: CVE-2021-38323
CVSS Score: 6.1 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
Researcher/s: p7e4
Fully Patched Version: No patch available, plugin closed for download.
Recommended Remediation: Uninstall Plugin.
Publication Date: 2021-09-08

The RentPress WordPress plugin is vulnerable to Reflected Cross-Site Scripting via the `selections` parameter found in the ~/src/rentPress/AjaxRequests.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 6.6.4.

Twitter Friends Widget <= 3.1 Reflected Cross-Site Scripting

Affected Plugin: Twitter Friends Widget
Plugin Slug: twitter-friends-widget
Affected Versions: <= 3.1
CVE ID: CVE-2021-38322
CVSS Score: 6.1 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
Researcher/s: p7e4
Fully Patched Version: No patch available, plugin closed for download.
Recommended Remediation: Uninstall Plugin.
Publication Date: 2021-09-08

The Twitter Friends Widget WordPress plugin is vulnerable to Reflected Cross-Site Scripting via the `pmc_TF_user` and `pmc_TF_password` parameter found in the ~/twitter-friends-widget.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 3.1.

Custom Menu Plugin <= 1.3.3 Reflected Cross-Site Scripting

Affected Plugin: Custom Menu Plugin
Plugin Slug: custom-sub-menus
Affected Versions: <= 1.3.3

CVE ID: CVE-2021-38321
CVSS Score: 6.1 (Medium)

Recommended Remediation: Uninstall Plugin.
Publication Date: 2021-09-08

The Custom Menu Plugin WordPress plugin is vulnerable to Reflected Cross-Site Scripting via the `selected_menu` parameter found in the ~/custom-menus.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 1.3.3.

---

simpleSAMLphp Authentication <= 0.7.0 Reflected Cross-Site Scripting

Affected Plugin: simpleSAMLphp Authentication
Plugin Slug: simplesamlphp-authentication
Affected Versions: <= 0.7.0
CVE ID: CVE-2021-38320
CVSS Score: 6.1 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
Researcher/s: p7e4
Fully Patched Version: No patch available, plugin closed for download.
Recommended Remediation: Uninstall Plugin.
Publication Date: 2021-09-08

The simpleSAMLphp Authentication WordPress plugin is vulnerable to Reflected Cross-Site Scripting due to a reflected `$_SERVER["PHP_SELF"]` value in the ~/simplesamlphp-authentication.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 0.7.0.

More From Google <= 0.0.2 Reflected Cross-Site Scripting

Affected Plugin: More From Google
Plugin Slug: more-from-google
Affected Versions: <= 0.0.2
CVE ID: CVE-2021-38319
CVSS Score: 6.1 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
Researcher/s: p7e4
Fully Patched Version: No patch available, plugin closed for download.
Recommended Remediation: Uninstall Plugin.
Publication Date: 2021-09-08

The More From Google WordPress plugin is vulnerable to Reflected Cross-Site Scripting due to a reflected `$_SERVER["PHP_SELF"]` value in the ~/morefromgoogle.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 0.0.2.

3D Cover Carousel <= 1.0 Reflected Cross-Site Scripting

Affected Plugin: 3D Cover Carousel
Plugin Slug: 3d-cover-carousel
Affected Versions: <= 1.0
CVE ID: CVE-2021-38318
CVSS Score: 6.1 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
Researcher/s: p7e4
Fully Patched Version: No patch available, plugin closed for download.
Recommended Remediation: Uninstall Plugin.
Publication Date: 2021-09-08

The 3D Cover Carousel WordPress plugin is vulnerable to Reflected Cross-Site Scripting via the `id` parameter in the ~/cover-carousel.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 1.0.

Konnichiwa! Membership <= 0.8.3 Reflected Cross-Site Scripting

Affected Plugin: Konnichiwa! Membership
Plugin Slug: konnichiwa
Affected Versions: <= 0.8.3
CVE ID: CVE-2021-38317
CVSS Score: 6.1 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
Researcher/s: p7e4
Fully Patched Version: No patch available, plugin closed for download.
Recommended Remediation: Uninstall Plugin.
Publication Date: 2021-09-08

The Konnichiwa! Membership WordPress plugin is vulnerable to Reflected Cross-Site Scripting via the `plan_id` parameter in the ~/views/subscriptions.html.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 0.8.3.

WP Academic People List <= 0.4.1 Reflected Cross-Site Scripting

Affected Plugin: WP Academic People List
Plugin Slug: wp-academic-people
Affected Versions: <= 0.4.1
CVE ID: CVE-2021-38316
CVSS Score: 6.1 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
Researcher/s: p7e4
Fully Patched Version: No patch available, plugin closed for download.
Recommended Remediation: Uninstall Plugin.
Publication Date: 2021-09-08

The WP Academic People List WordPress plugin is vulnerable to Reflected Cross-Site Scripting via the `category_name` parameter in the ~/admin-panel.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 0.4.1.

Gutenberg Template Library & Redux Framework <= 4.2.11 Sensitive Information Disclosure

Affected Plugin: Gutenberg Template Library & Redux Framework
Plugin Slug: redux-framework
Affected Versions: <= 4.2.11
CVE ID: CVE-2021-38314
CVSS Score: 5.3 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
Researcher/s: Ram Gall
Fully Patched Version: 4.2.13
Recommended Remediation: Update to version 4.2.13, or newer.
Publication Date: 2021-09-01

The Gutenberg Template Library & Redux Framework plugin <= 4.2.11 for WordPress registered several AJAX actions available to unauthenticated users in the `includes` function in `redux-core/class-redux-core.php` that were unique to a given site but deterministic and predictable given that they were based on an md5 hash of the site URL with a known salt value of '-redux' and an md5 hash of the previous hash with a known salt value of '-support'. These AJAX actions could be used to retrieve a list of active plugins and their versions, the site's PHP version, and an unsalted md5 hash of site's `AUTH_KEY` concatenated with the `SECURE_AUTH_KEY`. Read More Here.

Gutenberg Template Library & Redux Framework <= 4.2.11 Incorrect Authorization Check to Arbitrary Plugin Installation and Post Deletion

Affected Plugin: Gutenberg Template Library & Redux Framework
Plugin Slug: redux-framework
Affected Versions: <= 4.2.11
CVE ID: CVE-2021-38312
CVSS Score: 7.1 (High)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:L
Researcher/s: Ram Gall
Fully Patched Version: 4.2.13
Recommended Remediation: Update to version 4.2.13, or newer.
Publication Date: 2021-09-01

The Gutenberg Template Library & Redux Framework plugin <= 4.2.11 for WordPress used an incorrect authorization check in the REST API endpoints registered under the "redux/v1/templates/" REST Route in "redux-templates/classes/class-api.php".
The `permissions_callback` used in this file only checked for the `edit_posts` capability which is granted to lower-privileged users such as contributors, allowing such users to install arbitrary plugins from the WordPress repository and edit arbitrary posts. Read More Here.

Easy Social Icons <= 3.0.8 – Reflected Cross-Site Scripting

Affected Plugin: Easy Social Icons
Plugin Slug: easy-social-icons
Affected Versions: <= 3.0.8
CVE ID: CVE-2021-39322
CVSS Score: 6.1 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
Researcher/s: Ram Gall
Fully Patched Version: 3.0.9
Recommended Remediation: Update to version 3.0.9, or newer.
Publication Date: 2021-09-01

The Easy Social Icons plugin <= 3.0.8 for WordPress echoes out the raw value of `$_SERVER['PHP_SELF']` in its main file. On certain configurations including Apache+modPHP this makes it possible to use it to perform a reflected Cross-Site Scripting attack by injecting malicious code in the request path.

underConstruction <= 1.18 – Reflected Cross-Site Scripting

Affected Plugin: underConstruction
Plugin Slug: underconstruction
Affected Versions: <= 1.18
CVE ID: CVE-2021-39320
CVSS Score: 6.1 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
Researcher/s: Ram Gall
Fully Patched Version: 1.19
Recommended Remediation: Update to version 1.19, or newer.
Publication Date: 2021-08-31

The underConstruction plugin <= 1.18 for WordPress echoes out the raw value of `$GLOBALS['PHP_SELF']` in the ucOptions.php file. On certain configurations including Apache+modPHP, this makes it possible to use it to perform a reflected Cross-Site Scripting attack by injecting malicious code in the request path.

DZS Zoomsounds <= 6.45 Unauthenticated Directory Traversal

Affected Plugin: DZS Zoomsounds
Plugin Slug: dzs-zoomsounds
Affected Versions: <= 6.45
CVE ID: CVE-2021-39316
CVSS Score: 7.5 (High)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
Researcher/s: DigitalJessica Ltd
Fully Patched Version: 6.50
Recommended Remediation: Update to version 6.50 or newer.
Publication Date: 2021-08-30

The Zoomsounds plugin <= 6.45 for WordPress allows arbitrary files, including sensitive configuration files such as wp-config.php, to be downloaded via the `dzsap_download` action using directory traversal in the `link` parameter.

Nested Pages <= 3.1.15 Open Redirect

Affected Plugin: Nested Pages
Plugin Slug: wp-nested-pages
Affected Versions: <= 3.1.15
CVE ID: CVE-2021-38343
CVSS Score: 4.7 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:N/A:N
Researcher/s: Ram Gall
Fully Patched Version: 3.1.16
Recommended Remediation: Update to version 3.1.16 or newer.
Publication Date: 2021-08-25

The Nested Pages WordPress plugin <= 3.1.15 was vulnerable to an Open Redirect via the `page` POST parameter in the `npBulkActions`, `npBulkEdit`, `npListingSort`, and `npCategoryFilter` `admin_post` actions. Read more here.

Nested Pages <= 3.1.15 Cross-Site Request Forgery to Arbitrary Post Deletion and Modification

Affected Plugin: Nested Pages
Plugin Slug: wp-nested-pages
Affected Versions: <= 3.1.15
CVE ID: CVE-2021-38342
CVSS Score: 7.1 (High)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:H
Researcher/s: Ram Gall
Fully Patched Version: 3.1.16
Recommended Remediation: Update to version 3.1.16 or newer.
Publication Date: 2021-08-25

The Nested Pages WordPress plugin <= 3.1.15 was vulnerable to Cross-Site Request Forgery via the `npBulkActionS` and `npBulkEdit` `admin_post` actions, which allowed attackers to trash or permanently purge arbitrary posts as well as changing their status, reassigning their ownership, and editing other metadata. Read more here.

WordPress Real Media Library <= 4.14.1 Author-only Stored Cross-Site Scripting

Affected Plugin: WordPress Real Media Library
Plugin Slug: real-media-library-lite
Affected Versions: <= 4.14.1
CVE ID: CVE-2021-34668
CVSS Score: 6.4 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:N
Researcher/s: Thinkland Security Team
Fully Patched Version: 4.14.2
Recommended Remediation: Update to version 4.14.2 or newer.
Publication Date: 2021-08-25

The WordPress Real Media Library WordPress plugin is vulnerable to Stored Cross-Site Scripting via the `name` parameter in the ~/inc/overrides/lite/rest/Folder.php file which allows author-level attackers to inject arbitrary web scripts in folder names, in versions up to and including 4.14.1.

Booster for WooCommerce <= 5.4.3 Authentication Bypass

Affected Plugin: Booster For WooCommerce
Plugin Slug: woocommerce-jetpack
Affected Versions: <= 5.4.3
CVE ID: CVE-2021-34646
CVSS Score: 9.8 (Critical)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Researcher/s: Chloe Chamberland
Fully Patched Version: 5.4.4
Recommended Remediation: Update to version 5.4.4 or newer.
Publication Date: 2021-08-24

Versions up to, and including, 5.4.3, of the Booster for WooCommerce WordPress plugin are vulnerable to authentication bypass via the `process_email_verification` function due to a random token generation weakness in the `reset_and_mail_activation_link` function found in the ~/includes/class-wcj-emails-verification.php file. This allows attackers to impersonate users and trigger an email address verification for arbitrary accounts, including administrative accounts, and automatically be logged in as that user, including any site administrators. This requires the `Email Verification` module to be active in the plugin and the `Login User After Successful Verification` setting to be enabled, which it is by default. Read more here.

Shopping Cart & eCommerce Store <= 5.1.0 Cross-Site Request Forgery to Stored Cross-Site Scripting

Affected Plugin: Shopping Cart & eCommerce Store
Plugin Slug: wp-easycart

Affected Versions: <= 5.1.0
CVE ID: CVE-2021-34645

Fully Patched Version: No patch available, plugin closed for download.
Recommended Remediation: Uninstall Plugin.
Publication Date: 2021-08-18

The Shopping Cart & eCommerce Store WordPress plugin is vulnerable to Cross-Site Request Forgery via the `save_currency_settings` function found in the ~/admin/inc/wp_easycart_admin_initial_setup.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 5.1.0.

SP Project & Document Manager <= 4.25 Attribute-based Reflected Cross-Site Scripting

Affected Plugin: SP Project & Document Manager
Plugin Slug: sp-client-document-manager
Affected Versions: <= 4.25
CVE ID: CVE-2021-38315
CVSS Score: 6.1 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
Researcher/s: Thinkland Security Team
Fully Patched Version: No patch available, plugin closed for download.
Recommended Remediation: Uninstall Plugin.
Publication Date: 2021-08-16

The SP Project & Document Manager WordPress plugin is vulnerable to attribute-based Reflected Cross-Site Scripting via the `from` and `to` parameters in the ~/functions.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 4.25.

SEOPress 5.0.0 – 5.0.3 Authenticated Stored Cross-Site Scripting

Affected Plugin: SEOPress
Plugin Slug: wp-seopress
Affected Versions: 5.0.0 – 5.0.3
CVE ID: CVE-2021-34641
CVSS Score: 6.4 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:N
Researcher/s: Chloe Chamberland
Fully Patched Version: 5.0.4
Recommended Remediation: Update to version 5.0.4 or newer.
Publication Date: 2021-08-16

The SEOPress WordPress plugin is vulnerable to Stored Cross-Site-Scripting via the `processPut` function found in the ~/src/Actions/Api/TitleDescriptionMeta.php file which allows authenticated attackers to inject arbitrary web scripts, in versions 5.0.0 – 5.0.3. Read more here.

Calendar_plugin <= 1.0 Reflected Cross-Site Scripting

Affected Plugin: Calendar_plugin
Plugin Slug: calendar-plugin
Affected Versions: <= 1.0
CVE ID: CVE-2021-34667
CVSS Score: 6.1 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
Researcher/s: p7e4
Fully Patched Version: No patch available, plugin closed for download.
Recommended Remediation: Uninstall Plugin.
Publication Date: 2021-08-13

The Calendar_plugin WordPress plugin is vulnerable to Reflected Cross-Site Scripting due to the use of `$_SERVER['PHP_SELF']` in the ~/calendar.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 1.0.

Add Sidebar <= 2.0.0 Reflected Cross-Site Scripting

Affected Plugin: Add Sidebar
Plugin Slug: sidebar-adder
Affected Versions: <= 2.0.0
CVE ID: CVE-2021-34666
CVSS Score: 6.1 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
Researcher/s: p7e4
Fully Patched Version: No patch available, plugin closed for download.
Recommended Remediation: Uninstall Plugin.
Publication Date: 2021-08-13

The Add Sidebar WordPress plugin is vulnerable to Reflected Cross-Site Scripting via the `add` parameter in the ~/wp_sidebarMenu.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 2.0.0.

WP SEO Tags <= 2.2.7 Reflected Cross-Site Scripting

Affected Plugin: WP SEO Tags
Plugin Slug: wp-seo-tags
Affected Versions: <= 2.2.7
CVE ID: CVE-2021-34665
CVSS Score: 6.1 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
Researcher/s: p7e4
Fully Patched Version: No patch available, plugin closed for download.
Recommended Remediation: Uninstall Plugin.
Publication Date: 2021-08-13

The WP SEO Tags WordPress plugin is vulnerable to Reflected Cross-Site Scripting via the `saq_txt_the_filter` parameter in the ~/wp-seo-tags.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 2.2.7.

Moova for WooCommerce <= 3.5 Reflected Cross-Site Scripting

Affected Plugin: Moova for WooCommerce
Plugin Slug: moova-for-woocommerce
Affected Versions: <= 3.5
CVE ID: CVE-2021-34664
CVSS Score: 6.1 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
Researcher/s: p7e4
Fully Patched Version: No patch available, plugin closed for download.
Recommended Remediation: Uninstall Plugin.
Publication Date: 2021-08-13

The Moova for WooCommerce WordPress plugin is vulnerable to Reflected Cross-Site Scripting via the `lat` parameter in the ~/Checkout/Checkout.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 3.5.

---

jQuery Tagline Rotator <= 0.1.5 Reflected Cross-Site Scripting

Affected Plugin: jQuery Tagline Rotator
Plugin Slug: jquery-tagline-rotator
Affected Versions: <= 0.1.5
CVE ID: CVE-2021-34663
CVSS Score: 6.1 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
Researcher/s: p7e4
Fully Patched Version: No patch available, plugin closed for download.
Recommended Remediation: Uninstall Plugin.
Publication Date: 2021-08-13

The jQuery Tagline Rotator WordPress plugin is vulnerable to Reflected Cross-Site Scripting due to the use of `$_SERVER['PHP_SELF']` in the ~/jquery-tagline-rotator.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 0.1.5.

Plugmatter Pricing Table Lite <= 1.0.32 Reflected Cross-Site Scripting

Affected Versions: <= 1.0.32
CVE ID: CVE-2021-34659
CVSS Score: 6.1 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
Researcher/s: p7e4
Fully Patched Version: No patch available, plugin closed for download.
Recommended Remediation: Uninstall Plugin.
Publication Date: 2021-08-13

The Plugmatter Pricing Table Lite WordPress plugin is vulnerable to Reflected Cross-Site Scripting via the `email` parameter in the ~/license.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 1.0.32.

Simple Popup Newsletter <= 1.4.7 Reflected Cross-Site Scripting

Affected Plugin: Simple Popup Newsletter
Plugin Slug: simple-popup-newsletter
Affected Versions: <= 1.4.7
CVE ID: CVE-2021-34658
CVSS Score: 6.1 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
Researcher/s: p7e4
Fully Patched Version: No patch available, plugin closed for download.
Recommended Remediation: Uninstall Plugin.
Publication Date: 2021-08-13

The Simple Popup Newsletter WordPress plugin is vulnerable to Reflected Cross-Site Scripting due to the use of `$_SERVER['PHP_SELF']` in the ~/simple-popup-newsletter.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 1.4.7.

TypoFR <= 0.11 Reflected Cross-Site Scripting

Affected Plugin: TypoFR
Plugin Slug: typofr
Affected Versions: <= 0.11
CVE ID: CVE-2021-34657
CVSS Score: 6.1 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
Researcher/s: p7e4
Fully Patched Version: No patch available, plugin closed for download.
Recommended Remediation: Uninstall Plugin.
Publication Date: 2021-08-13

The 2TypoFR WordPress plugin is vulnerable to Reflected Cross-Site Scripting via the `text` function found in the ~/vendor/Org_Heigl/Hyphenator/index.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 0.11.

WP Songbook <= 2.0.11 Reflected Cross-Site Scripting

Affected Plugin: WP Songbook
Plugin Slug: wp-songbook
Affected Versions: <= 2.0.11
CVE ID: CVE-2021-34655
CVSS Score: 6.1 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
Researcher/s: p7e4
Fully Patched Version: No patch available, plugin closed for download.
Recommended Remediation: Uninstall Plugin.
Publication Date: 2021-08-13

The WP Songbook WordPress plugin is vulnerable to Reflected Cross-Site Scripting via the `url` parameter found in the ~/inc/class.ajax.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 2.0.11.

Custom Post Type Relations <= 1.0 Reflected Cross-Site Scripting

Affected Plugin: Custom Post Type Relations
Plugin Slug: custom-post-type-relations
Affected Versions: <= 1.0
CVE ID: CVE-2021-34654
CVSS Score: 6.1 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
Researcher/s: p7e4
Fully Patched Version: No patch available, plugin closed for download.
Recommended Remediation: Uninstall Plugin.
Publication Date: 2021-08-13

The Custom Post Type Relations WordPress plugin is vulnerable to Reflected Cross-Site Scripting via the `cptr[name]` parameter found in the ~/pages/admin-page.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 1.0.

2Way VideoCalls and Random Chat – HTML5 Webcam Videochat <= 5.2.7 Reflected Cross-Site Scripting

Affected Plugin: 2Way VideoCalls and Random Chat – HTML5 Webcam Videochat
Plugin Slug: webcam-2way-videochat
Affected Versions: <= 5.2.7
CVE ID: CVE-2021-34656
CVSS Score: 6.1 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
Researcher/s: p7e4
Fully Patched Version: No patch available, plugin closed for download.
Recommended Remediation: Uninstall Plugin.
Publication Date: 2021-08-13

The 2Way VideoCalls and Random Chat – HTML5 Webcam Videochat WordPress plugin is vulnerable to Reflected Cross-Site Scripting via the `vws_notice` function found in the ~/inc/requirements.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 5.2.7.

WP Fountain <= 1.5.9 Reflected Cross-Site Scripting

Affected Plugin:WP Fountain
Plugin Slug: wp-fountain
Affected Versions: <= 1.5.9
CVE ID: CVE-2021-34653
CVSS Score: 6.1 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
Researcher/s: p7e4
Fully Patched Version: No patch available, plugin closed for download.
Recommended Remediation: Uninstall Plugin.
Publication Date: 2021-08-13

The WP Fountain WordPress plugin is vulnerable to Reflected Cross-Site Scripting due to the use of `$_SERVER['PHP_SELF']` in the ~/wp-fountain.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 1.5.9.

Media Usage <= 0.0.4 Reflected Cross-Site Scripting

Affected Plugin: Media Usage
Plugin Slug: media-usage
Affected Versions: <= 0.0.4
CVE ID: CVE-2021-34652
CVSS Score: 6.1 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
Researcher/s: p7e4
Fully Patched Version: No patch available, plugin closed for download.
Recommended Remediation: Uninstall Plugin.
Publication Date: 2021-08-13

The Media Usage WordPress plugin is vulnerable to Reflected Cross-Site Scripting via the `id` parameter in the ~/mmu_admin.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 0.0.4.

Scribble Maps <= 1.2 Reflected Cross-Site Scripting

Affected Plugin: Scribble Maps
Plugin Slug: scribble-maps
Affected Versions: <= 1.2
CVE ID: CVE-2021-34651
CVSS Score: 6.1 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
Researcher/s: p7e4
Fully Patched Version: No patch available, plugin closed for download.
Recommended Remediation: Uninstall Plugin.
Publication Date: 2021-08-13

The Scribble Maps WordPress plugin is vulnerable to Reflected Cross-Site Scripting via the `map` parameter in the ~/includes/admin.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 1.2.

Simple Behance Portfolio <= 0.2 Reflected Cross-Site Scripting

Affected Plugin: Simple Behance Portfolio
Plugin Slug: simple-behace-portfolio
Affected Versions: <= 0.2
CVE ID: CVE-2021-34649
CVSS Score: 6.1 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
Researcher/s: p7e4
Fully Patched Version: No patch available, plugin closed for download.
Recommended Remediation: Uninstall Plugin.
Publication Date: 2021-08-13

The Simple Behance Portfolio WordPress plugin is vulnerable to Reflected Cross-Site Scripting via the `dark` parameter in the ~/titan-framework/iframe-font-preview.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 0.2.

Multiplayer Games <= 3.7 Reflected Cross-Site Scripting

Affected Plugin: Multiplayer Games
Plugin Slug: multiplayer-plugin
Affected Versions: <= 3.7
CVE ID: CVE-2021-34644
CVSS Score: 6.1 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
Researcher/s: p7e4
Fully Patched Version: No patch available, plugin closed for download.
Recommended Remediation: Uninstall Plugin.
Publication Date: 2021-08-13

The Multiplayer Games WordPress plugin is vulnerable to Reflected Cross-Site Scripting due to the use of `$_SERVER['PHP_SELF']` in the ~/multiplayergames.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 3.7.

Skaut bazar <= 1.3.2 Reflected Cross-Site Scripting

Affected Plugin: Skaut bazar
Plugin Slug: skaut-bazar
Affected Versions: <= 1.3.2
CVE ID: CVE-2021-34643
CVSS Score: 6.1 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
Researcher/s: p7e4
Fully Patched Version: No patch available, plugin closed for download.
Recommended Remediation: Uninstall Plugin.
Publication Date: 2021-08-13

The Skaut bazar WordPress plugin is vulnerable to Reflected Cross-Site Scripting due to the use of `$_SERVER['PHP_SELF']` in the ~/skaut-bazar.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 1.3.2.

Smart Email Alerts <= 1.0.10 Reflected Cross-Site Scripting

Affected Plugin: Smart Email Alerts
Plugin Slug: smart-email-alerts
Affected Versions: <= 1.0.10
CVE ID: CVE-2021-34642
CVSS Score: 6.1 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
Researcher/s: p7e4
Fully Patched Version: No patch available, plugin closed for download.
Recommended Remediation: Uninstall Plugin.
Publication Date: 2021-08-13

The Smart Email Alerts WordPress plugin is vulnerable to Reflected Cross-Site Scripting via the `api_key` in the ~/views/settings.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 1.0.10.

Securimage-WP-Fixed <= 3.5.4 – Reflected Cross-Site Scripting

Affected Plugin: Securimage-WP-Fixed
Plugin Slug: securimage-wp-fixed
Affected Versions: <= 3.5.4
CVE ID: CVE-2021-34640
CVSS Score: 6.1 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
Researcher/s: p7e4
Fully Patched Version: No patch available, plugin closed for download.
Recommended Remediation: Uninstall Plugin.
Publication Date: 2021-08-11

The Securimage-WP-Fixed WordPress plugin is vulnerable to Reflected Cross-Site Scripting due to the use of `$_SERVER['PHP_SELF']` in the ~/securimage-wp.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 3.5.4.

WP Fusion Lite <= 3.37.18 – Cross-Site Request Forgery to Data Deletion

Affected Plugin: WP Fusion Lite
Plugin Slug: wp-fusion-lite
Affected Versions: <= 3.37.18
CVE ID: CVE-2021-34661
CVSS Score: 6.1 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:L/A:L
Researcher/s: Xu-Liang Liao
Fully Patched Version: 3.37.30
Recommended Remediation: Update to version 3.37.30, or newer.
Publication Date: 2021-08-06

The WP Fusion Lite WordPress plugin is vulnerable to Cross-Site Request Forgery via the `show_logs_section` function found in the ~/includes/admin/logging/class-log-handler.php file which allows attackers to drop all logs for the plugin, in versions up to and including 3.37.18.

WP Fusion Lite <= 3.37.18 – Reflected Cross-Site Scripting

Affected Plugin: WP Fusion Lite
Plugin Slug: wp-fusion-lite
Affected Versions: <= 3.37.18
CVE ID: CVE-2021-34660
CVSS Score: 6.1 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
Researcher/s: Xu-Liang Liao
Fully Patched Version: 3.37.30
Recommended Remediation: Update to version 3.37.30, or newer.
Publication Date: 2021-08-06

The WP Fusion Lite WordPress plugin is vulnerable to Reflected Cross-Site Scripting via the `startdate` parameter found in the ~/includes/admin/logging/class-log-table-list.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 3.37.18.

Nifty Newsletters <= 4.0.23 – Cross-Site Request Forgery to Stored Cross-Site Scripting

Affected Plugin: Nifty Newsletters
Plugin Slug: sola-newsletters
Affected Versions: <= 4.0.23
CVE ID: CVE-2021-34634
CVSS Score: 8.8(High)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
Researcher/s: Kohei Hino, Cryptography Laboratory in Tokyo Denki University
Fully Patched Version: No patch available, plugin closed for download.
Recommended Remediation: Uninstall Plugin.
Publication Date: 2021-07-30

The Nifty Newsletters WordPress plugin is vulnerable to Cross-Site Request Forgery via the `sola_nl_wp_head` function found in the ~/sola-newsletters.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 4.0.23.

Youtube Feeder <= 2.0.1 – Cross-Site Request Forgery to Stored Cross-Site Scripting

Affected Plugin: Youtube Feeder
Plugin Slug: youtube-feeder
Affected Versions: <= 2.0.1
CVE ID: CVE-2021-34633
CVSS Score: 8.8 (High)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
Researcher/s: Kohei Hino, Cryptography Laboratory in Tokyo Denki University
Fully Patched Version: No patch available, plugin closed for download.
Recommended Remediation: Uninstall Plugin.
Publication Date: 2021-07-30

The Youtube Feeder WordPress plugin is vulnerable to Cross-Site Request Forgery via the `printAdminPage` function found in the ~/youtube-feeder.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 2.0.1.

WordPress Download Manager <= 3.1.24 Authenticated Arbitrary File Upload

Affected Plugin: WordPress Download Manager
Plugin Slug: download-manager
Affected Versions: <= 3.1.24
CVE ID: CVE-2021-34639
CVSS Score: 7.5 (High)
CVSS Vector: CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H
Researcher/s: Ramuel Gall
Fully Patched Version: 3.1.25
Recommended Remediation: Update to version 3.1.25 or newer.
Publication Date: 2021-07-29

Authenticated Arbitrary File Upload in WordPress Download Manager <= 3.1.24 allows authenticated (Author+) users to upload files with a double extension, e.g. "payload.php.png". The destination folder is protected by an .htaccess file so most configurations are not vulnerable. Read more here.

WordPress Download Manager <= 3.1.24 Authenticated Directory Traversal

Affected Plugin: WordPress Download Manager
Plugin Slug: download-manager
Affected Versions: <= 3.1.24
CVE ID: CVE-2021-34638
CVSS Score: 6.5 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N
Researcher/s: Ramuel Gall
Fully Patched Version: 3.1.25
Recommended Remediation: Update to version 3.1.25 or newer.
Publication Date: 2021-07-29

Authenticated Directory Traversal in WordPress Download Manager <= 3.1.24 allows authenticated (Contributor+) users to obtain sensitive configuration file information, as well as allowing Author+ users to perform XSS attacks by setting Download template to an uploaded JavaScript with an image extension. Read more here.

Post Index <= 0.7.5 Cross-Site Request Forgery to Stored Cross-Site Scripting

Affected Plugin: Post Index
Plugin Slug: post-index
Affected Versions: <= 0.7.5
CVE ID: CVE-2021-34637
CVSS Score: 8.8 (High)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
Researcher/s: Kentaro Kuroki, Cryptography Laboratory in Tokyo Denki University
Fully Patched Version: No patch available, plugin closed for download.
Recommended Remediation: Uninstall plugin.
Publication Date: 2021-07-26

The Post Index WordPress plugin is vulnerable to Cross-Site Request Forgery via the `OptionsPage` function found in the ~/php/settings.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 0.7.5.

Poll Maker <= 3.2.8 – Reflected Cross-Site Scripting

Affected Plugin: Poll Maker
Plugin Slug: poll-maker
Affected Versions: <=3.2.8
CVE ID: CVE-2021-34635
CVSS Score: 6.1 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
Researcher/s: Xu-Liang Liao
Fully Patched Version: 3.2.9
Recommended Remediation: Update to version 3.2.9 or newer.
Publication Date: 2021-07-26

The Poll Maker WordPress plugin is vulnerable to Reflected Cross-Site Scripting via the `mcount` parameter found in the ~/admin/partials/settings/poll-maker-settings.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 3.2.8.

SEO Backlinks <= 4.0.1 – Cross-Site Request Forgery to Stored Cross-Site Scripting

Affected Plugin: SEO Backlinks
Plugin Slug: seo-backlinks
Affected Versions: <= 4.0.1
CVE ID: CVE-2021-34632
CVSS Score: 8.8 (High)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
Researcher/s: Takahiro Yamashita, Cryptography Laboratory in Tokyo Denki University
Fully Patched Version: No patch available, plugin closed for download.
Recommended Remediation: Uninstall plugin.
Publication Date: 2021-07-26

The SEO Backlinks WordPress plugin is vulnerable to Cross-Site Request Forgery via the `loc_config` function found in the ~/seo-backlinks.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 4.0.1.

Admin Custom Login <= 3.2.7 – Cross-Site Request Forgery to Stored

Affected Plugin: Admin Custom Login
Plugin Slug: admin-custom-login
Affected Versions: <= 3.2.7
CVE ID: CVE-2021-34628
CVSS Score: 8.8 (High)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
Researcher/s: Ryoma Nishioka, Cryptography Laboratory in Tokyo Denki University
Fully Patched Version: 3.2.8
Recommended Remediation: Update to version 3.2.8 or newer.
Publication Date: 2021-07-26

The Admin Custom Login WordPress plugin is vulnerable to Cross-Site Request Forgery due to the `loginbgSave` action found in the ~/includes/Login-form-setting/Login-form-background.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 3.2.7.

GTranslate <= 2.8.64 – Reflected Cross-Site Scripting

Affected Plugin: GTranslate
Plugin Slug: gtranslate
Affected Versions: <= 2.8.64
CVE ID: CVE-2021-34630
CVSS Score: 5.0 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L
Researcher/s: N/A
Fully Patched Version: 2.8.65
Recommended Remediation: Update to the latest version available.
Publication Date: 2021-07-23

In the Pro and Enterprise versions of GTranslate < 2.8.65, the `gtranslate_request_uri_var` function runs at the top of all pages and echoes out the contents of `$_SERVER['REQUEST_URI']`. Although this uses addslashes, and most modern browsers automatically URLencode requests, this plugin is still vulnerable to Reflected XSS in older browsers such as Internet Explorer 9 or below, or in cases where an attacker is able to modify the request en route between the client and the server, or in cases where the user is using an atypical browsing solution.

NewsPlugin <= 1.0.18 – Cross-Site Request Forgery to Stored Cross-Site Scripting

Affected Plugin: NewsPlugin
Plugin Slug: newsplugin
Affected Versions: <= 1.0.18
CVE ID: CVE-2021-34631
CVSS Score: 8.8 (High)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
Researcher/s: Taichi Ichimura, Cryptography Laboratory in Tokyo Denki University
Fully Patched Version: No patch available, plugin closed for download.
Recommended Remediation: Uninstall plugin.
Publication Date: 2021-07-21

The NewsPlugin WordPress plugin is vulnerable to Cross-Site Request Forgery via the `handle_save_style` function found in the ~/news-plugin.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 1.0.18.

SendGrid <= 1.11.8 – Authorization Bypass

Affected Plugin: SendGrid
Plugin Slug: sendgrid-email-delivery-simplified
Affected Versions: <= 1.11.8
CVE ID: CVE-2021-34629
CVSS Score: 4.3 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N
Researcher/s: Prashant Baldha
Fully Patched Version: No patch available, plugin closed for download.
Recommended Remediation: Uninstall plugin.
Publication Date: 2021-07-21

The SendGrid WordPress plugin is vulnerable to authorization bypass via the `get_ajax_statistics` function found in the ~/lib/class-sendgrid-statistics.php file which allows authenticated users to export statistics for a WordPress multi-site main site, in versions up to and including 1.11.8. This vulnerability only affects the main site of WordPress multi-site installations.

WP Upload Restriction <= 2.2.3 – Authenticated Stored Cross-Site Scripting

Affected Plugin: WP Upload Restriction
Plugin Slug: wp-upload-restriction
Affected Versions: <= 2.2.3
CVE ID: CVE-2021-34625
CVSS Score: 6.4 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:N
Researcher/s: Angelo Righi
Fully Patched Version: No patch available, plugin closed for download.
Recommended Remediation: Uninstall plugin.

Missing Access Control in the `saveCustomType` function allows for authenticated users, such as subscribers, to add mime types and extensions through unsanitized parameters that makes it possible to inject malicious web scripts that later execute when an administrator visits the extensions page.

WP Upload Restriction <= 2.2.3 – Missing Access Control in deleteCustomType function

Affected Plugin: WP Upload Restriction
Plugin Slug: wp-upload-restriction
Affected Versions: <= 2.2.3
CVE ID: CVE-2021-34626
CVSS Score: 4.3 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N
Researcher/s: N/A
Fully Patched Version: No patch available, plugin closed for download.
Recommended Remediation: Uninstall plugin.

Missing access control in `deleteCustomType` function allows authenticated users, such as subscribers, to delete custom extensions.

WP Upload Restriction <= 2.2.3 – Missing Access Control in getSelectedMimeTypesByRole function

Affected Plugin: WP Upload Restriction
Plugin Slug: wp-upload-restriction
Affected Versions: <= 2.2.3
CVE ID: CVE-2021-34627
CVSS Score: 4.3 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N
Researcher/s: N/A
Fully Patched Version: No patch available, plugin closed for download.
Recommended Remediation: Uninstall plugin.

Missing access control in `getSelectedMimeTypesByRole` function allows authenticated users, such as subscribers, to retrieve approved mime types for any given role.

ProfilePress 3.0 – 3.1.3 – Unauthenticated Privilege Escalation

Affected Plugin: User Registration, User Profiles, Login & Membership – ProfilePress (Formerly WP User Avatar)
Plugin Slug: wp-user-avatar
Affected Versions: 3.0 – 3.1.3
CVE ID: CVE-2021-34621
CVSS Score: 9.8 (CRITICAL)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Researcher/s: Chloe Chamberland
Fully Patched Version: 3.1.4

possible for anyone to register as an administrator. More details.

ProfilePress 3.0 – 3.1.3 – Authenticated Privilege Escalation

Affected Plugin: User Registration, User Profiles, Login & Membership – ProfilePress (Formerly WP User Avatar)
Plugin Slug: wp-user-avatar
Affected Versions: 3.0 – 3.1.3
CVE ID: CVE-2021-34622
CVSS Score: 9.8 (CRITICAL)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Researcher/s: Chloe Chamberland
Fully Patched Version: 3.1.4
Recommended Remediation: Update to version 3.1.4 or newer

During user profile updates, users could supply arbitrary user meta data that would get updated making it possible for anyone to escalate their privileges to that of an administrator. More details.

ProfilePress 3.0 – 3.1.3 – Arbitrary File Upload in Image Uploader Component

Affected Plugin: User Registration, User Profiles, Login & Membership – ProfilePress (Formerly WP User Avatar)
Plugin Slug: wp-user-avatar
Affected Versions: 3.0 – 3.1.3
CVE ID: CVE-2021-34623
CVSS Score: 9.8 (CRITICAL)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Researcher/s: Chloe Chamberland
Fully Patched Version: 3.1.4
Recommended Remediation: Update to version 3.1.4 or newer

The image uploader component used to upload profile photos and user cover photos was vulnerable to arbitrary file uploads due to insufficient file type validation. More details.

ProfilePress 3.0 – 3.1.3 – Arbitrary File Upload in File Uploader Component

Affected Plugin: User Registration, User Profiles, Login & Membership – ProfilePress (Formerly WP User Avatar)
Plugin Slug: wp-user-avatar
Affected Versions: 3.0- 3.1.3
CVE ID: CVE-2021-34624
CVSS Score: 9.8 (CRITICAL)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Researcher/s: Chloe Chamberland
Fully Patched Version: 3.1.4
Recommended Remediation: Update to version 3.1.4 or newer

The file uploader component used to upload files during registration was vulnerable to arbitrary file uploads due to insufficient file type validation. More details.

WP Fluent Forms <= 3.6.65 – CSRF to Stored XSS

Affected Plugin: WP Fluent Forms
Plugin Slug: fluentform
Affected Versions: < 3.6.67
CVE ID: CVE-2021-34620
CVSS Score: 7.1 (High)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:L
Researcher/s: Ramuel Gall
Fully Patched Version: 3.6.67
Recommended Remediation: Update to version 3.6.67 or newer.

This plugin is vulnerable to Cross-Site Request Forgery leading to stored Cross-Site Scripting and limited Privilege Escalation due to a missing nonce check in the access control function for administrative AJAX actions. More details.

Woocommerce Stock Manager <= 2.5.7 – CSRF to Arbitrary File Upload

Affected Plugin: WooCommerce Stock Manager
Plugin Slug: woocommerce-stock-manager
Affected Versions: <= 2.5.7
CVE ID: CVE-2021-34619
CVSS Score: 8.8 (HIGH)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
Researcher/s: Chloe Chamberland
Fully Patched Version: 2.6.0
Recommended Remediation: Update to version 2.6.0 or newer.

This plugin is vulnerable to Cross-Site Request Forgery leading to Arbitrary File Upload due to missing nonce and file validation in the /woocommerce-stock-manager/trunk/admin/views/import-export.php file. More details.