< Back to all zero days

Stored Cross-Site Scripting in WordPress [Post Duplicator Plugin - 2.23]

AFFECTED VENDOR	STATUS	DATE
WordPress	Fixed	Dec 2, 2021

Description Proof of concept (POC) Impact Remediations Timeline

Description

A cross-site scripting (XSS) attack can cause arbitrary code (javascript) to run in a user's browser while the browser is connected to a trusted website. The application targets your application's users and not the application itself, but it uses your application as the vehicle for the attack. The XSS payload executes whenever the user opens the Settings Page of the Post Duplicator Plugin or the application root page after duplicating any of the existing posts.

Affected Vendor
WordPress

Bug Name
Stored Cross-Site Scripting

CVE Number
CVE-2021-33852

CWE ID
CWE-79

CSW ID
2021-CSW-12-1053

CVSSv3 Score
6.1

Affected Version
Plugin - 2.23

Severity
Medium

Affected Product
Post-Duplicator Plugin 2.23

Proof of concept: (POC)

The following vulnerability was discovered in Post-Duplicator Plugin 2.23.

Issue: Stored Cross-Site Scripting

Note: Here, localhost has been used for testing the application locally.

1. Login to the WordPress application.
2. Install Post Duplicator Plugin.
3. Go to the 'Tools' menu of WordPress and click on the 'Post Duplicator' button.

Figure 01: *Post Duplicator Settings Page*

4. Enter the payload - Duplicate Post"><script>alert(document.cookie)</script> in the 'Duplicate Title' field (mtphr_post_duplicator_settings[title] parameter).

Figure 02: *Entering XSS payload in the 'Duplicate Title' field*

5. Enter the payload - Hello World!"><script>alert(document.cookie)</script> in the 'Duplicate Slug' field (mtphr_post_duplicator_settings[slug] parameter).

Figure 03: *Entering XSS payload in the 'Duplicate Slug' field*

6. Click on the 'Save Changes' button to save changes.
7. Go to the Post Duplicator Settings page at tools.php?page=mtphr_post_duplicator_settings_menu

***Figure 04**: Injected XSS payload is executed displaying an alert box with the contents of the user's cookies.*

8. Another use case of this vulnerability is when the post is duplicated after injecting the XSS payload in the settings page.

***Figure 05**: Duplicate the "Hello world!" post*

9. Once the post is duplicated, the title of the duplicated post will append the name we specified in the mtphr_post_duplicator_settings[title] parameter.

***Figure 06**: Duplicated post with XSS Payload*

10. Now navigate to the application root to view the posts.

***Figure 07**: Injected XSS payload is executed displaying an alert box with the contents of the user's cookies.*

***Figure 08**: The default cross-site scripting mitigation setting in wp.config file to prevent cross-site scripting attacks*

Impact

An attacker can perform the following:

- Inject malicious code into the vulnerable variable and exploit the application through the cross-site scripting vulnerability.
- Modify the code and get the session information of other users
- Compromise the user machine.

Remediations

- Perform context-sensitive encoding of entrusted input before it is echoed back to a browser using an encoding library throughout the application.
- Implement input validation for special characters on all the variables reflected in the browser and stored in the database.
- Explicitly set the character set encoding for each page generated by the webserver.
- Encode dynamic output elements and filter specific characters in dynamic elements.

Timeline

Dec 28, 2021: Discovered in 'Post Duplicator Pluqin – 2.23' Product

-33852)

Additional Notes

Security Advisory Published by WordPress

Discovered by

Cyber Security Works Pvt. Ltd.

Talk to CSW's team of experts to secure your landscape.

Schedule free consultation

Cyber Security Works helps reduce security debt and inherent vulnerabilities in an organization's infrastructure and code. We work with large public, private, and start-up companies and help them prioritize their vulnerabilities.

Resources

- Ransomware
- Cyber Risk Series
- Blogs
- Patch Watch
- Data Sheets
- White Papers
- Zero Days
- Glossary
- Events
- CISA-KEV

Partner

- Become a Partner

Quick Links

- About Us
- Contact Us
- Careers
- Services
- Media Coverage
- Cybersecurity month
- Predictions for 2022
- Cybersecurity for govt
- Hackathon