

Stored Cross Site Scripting (XSS) in parameter rp4wp[heading_text] in barrykooij/related-posts-for-wp

**Valid**

Reported on Oct 5th 2022

Description

The Related Posts for WordPress plugin is vulnerable to stored XSS, specifically in the rp4wp[heading_text] parameter because the user input is not properly sanitized, allowing the insertion of JavaScript code that can exploit the vulnerability.

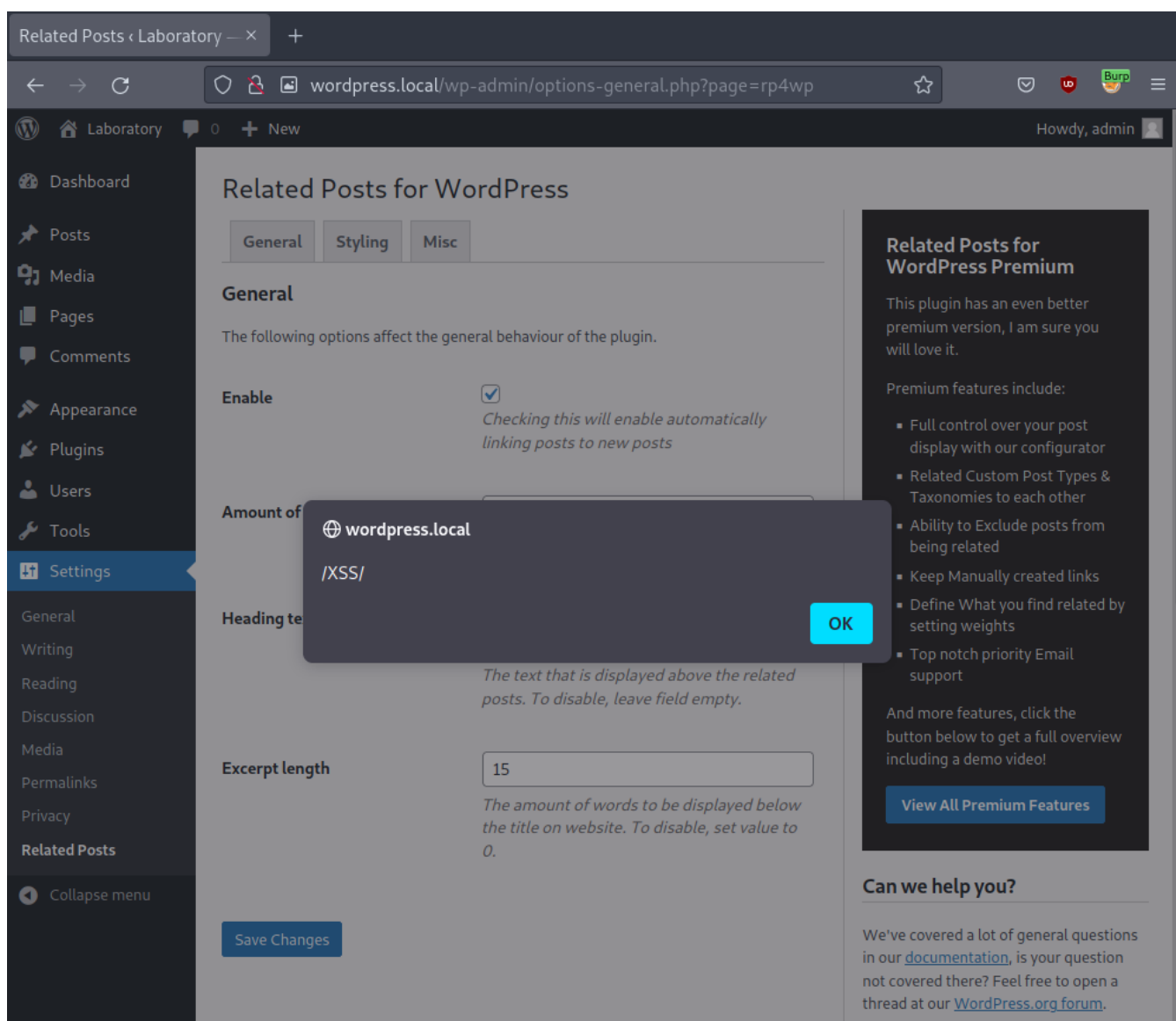
Proof of Concept

- 1 - Install and activate version 2.1.2 of the plugin.
- 2 - Go to the plugin settings panel ([http://\[TARGET\]/wp-admin/options-general.php?page=rp4wp](http://[TARGET]/wp-admin/options-general.php?page=rp4wp)).
- 3 - Insert the following payload in the "Heading text" field:

```
" autofocus onfocus=alert(/XSS/)>
```

- 4 - Save the changes and immediately the popup window demonstrating the vulnerability (PoC) will be executed.

Evidence



Impact

This vulnerability would potentially allow attackers to hijack the user's current session, steal relevant information, deface the website or direct users to malicious websites, and there is even the possibility of escalating the level of exploitation or more advanced attacks (for example, create privileged users on the WordPress instance, upload a backdoor or even establish a reverse connection).

Occurrences

 class-settings.php L212

Chat with us

CVE

CVE-2022-3506

(Published)

Vulnerability Type

CWE-79: Cross-site Scripting (XSS) - Stored

Severity

Medium (5.5)

Registry

Other

Affected Version

2.1.2

Visibility

Public

Status

Fixed

Found by

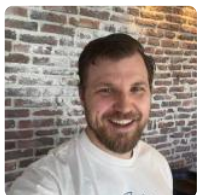


Juampa Rodríguez

@und3sc0n0c1d0

legend ▼

Fixed by



Barry Kooij

@barrykooij

unranked ▼

This report was seen 834 times.

We are processing your report and will contact the **barrykooij/related-posts-for-wp** team within 24 hours. 2 months ago

We have contacted a member of the **barrykooij/related-posts-for-wp** team and are waiting to hear back. 2 months ago

We have sent a follow up to the **barrykooij/related-posts-for-wp** team. We will try again in 7 days. 2 months ago

Chat with us

days. 2 months ago

Barry Kooij validated this vulnerability 2 months ago

Juampa Rodríguez has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

Juampa 2 months ago

Researcher

@maintainer Is it okay with you if I am assigned a CVE for this vulnerability?

We have sent a fix follow up to the **barrykooij/related-posts-for-wp** team. We will try again in 7 days. a month ago

Barry Kooij a month ago

Maintainer

@Juampa Rodríguez I'm not sure how to do that.

Barry Kooij a month ago

Maintainer

Fixed on master branch <https://github.com/barrykooij/related-posts-for-wp/commit/37733398dd88863fc0bdb3d6d378598429fd0b81>

Will release update later today.

Juampa a month ago

Researcher

@maintainer I will be happy to re-validate the vulnerability once I have the fixed version of your source code.

@admin, could you please provide me with a new CVE for this vulnerability?

Barry Kooij marked this as fixed in **2.1.3** with commit **377333** a month ago

Barry Kooij has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

Chat with us

class-settings.php#L212 has been validated ✓

Barry Kooij published this vulnerability a month ago

Ben Harvie [a month ago](#)

[Admin](#)

This report has now been assigned a CVE as requested and it will publish momentarily. Happy hunting:)

Sign in to join this conversation

2022 © 418sec

huntr

home

hacktivity

leaderboard

FAQ

contact us

terms

privacy policy

part of 418sec

company

about

team

Chat with us