

New issue

[Jump to bottom](#)

Cross Site Scripting Vulnerability on "Menu Preferences" feature in Textpattern v4.8.1 #1495

🔒 Closed

luuthehienhbit opened this issue on Jun 8, 2020 · 2 comments

luuthehienhbit commented on Jun 8, 2020

Expected behaviour

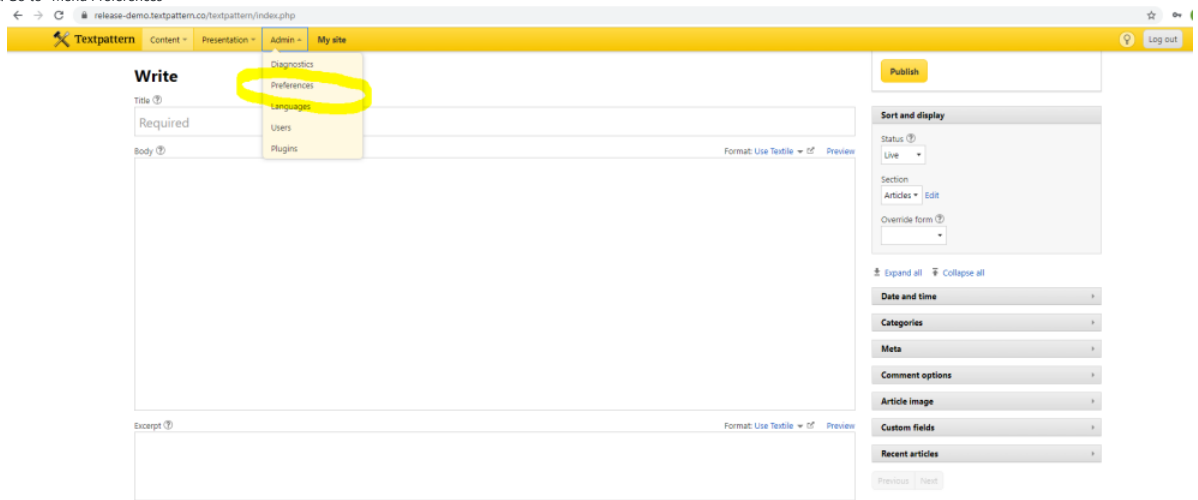
An authenticated malicious user can take advantage of a Stored XSS vulnerability in the "Menu Preferences" feature.

Impact

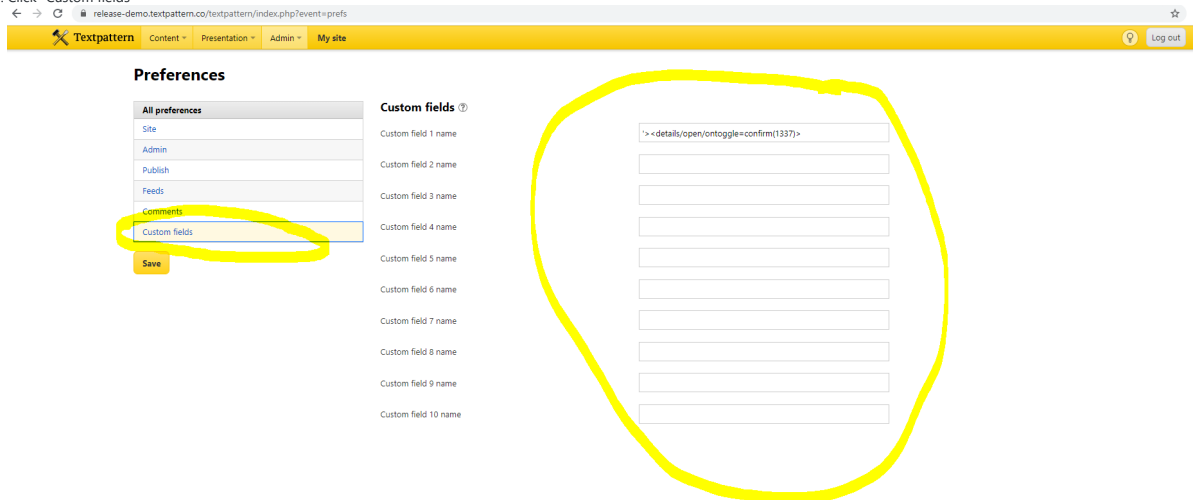
Commonly include transmitting private data, like cookies or other session information, to the attacker, redirecting the victim to web content controlled by the attacker, or performing other malicious operations on the user's machine under the guise of the vulnerable site.

Steps to reproduce

1. Log into the Admin.
2. Go to "Menu Preferences"



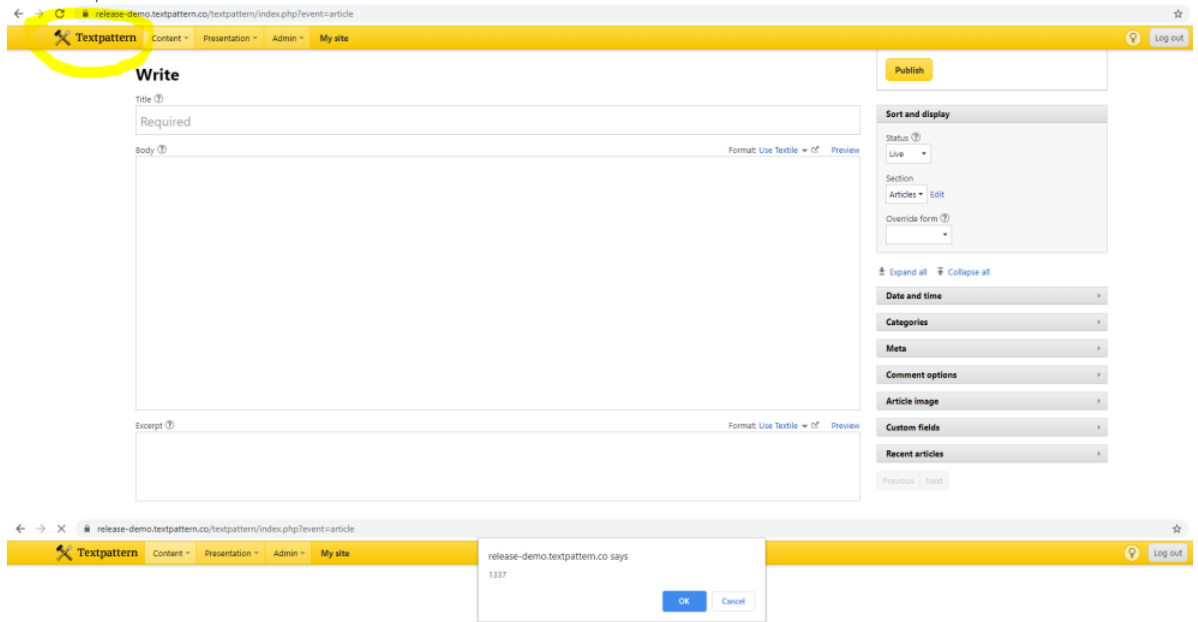
3. Click "Custom fields"



4. Insert payload to Fields name:

'<script>details/open/ontoggle=confirm(1337)</script>'

5. Click Icon Textpattern:



Additional information

Textpattern version: 4.8.1

 **Bloke** closed this as completed in [8623928](#) on Jun 8, 2020

Bloke commented on Jun 8, 2020

Member


Thank you for the report. Although it's a low-level vector (since the only people that can set Custom Field labels are Managing Editors and higher, whom should be inherently trusted), sanitizing the label is good practice as they're not supposed to contain any dubious characters.


This is now fixed in the upcoming 4.8.2 release in commit [8623928](#). Please test and ensure it has no unintended consequences.

 1

luuthehienhbit commented on Jun 8, 2020

Author

Hi Bloke.
I will continue testing with your product.
You can a CVE ID assigned and reference change log to "UraSec Team" 
Thanks you!

 **Bloke** added a commit that referenced this issue on Jul 11, 2020

 Sanitize custom field label ...

92d7f2c

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants

