



Tanmay Bhattacharjee

Follow

Sep 3, 2021 · 1 min read · Listen



Textpattern 4.8.7 is affected by HTML injection in the Body parameter.

#Exploit Title: Textpattern CMS v4.8.7 "Content>Write>Body" — HTMLI

Exploit Author: Tanmay Bhattacharjee

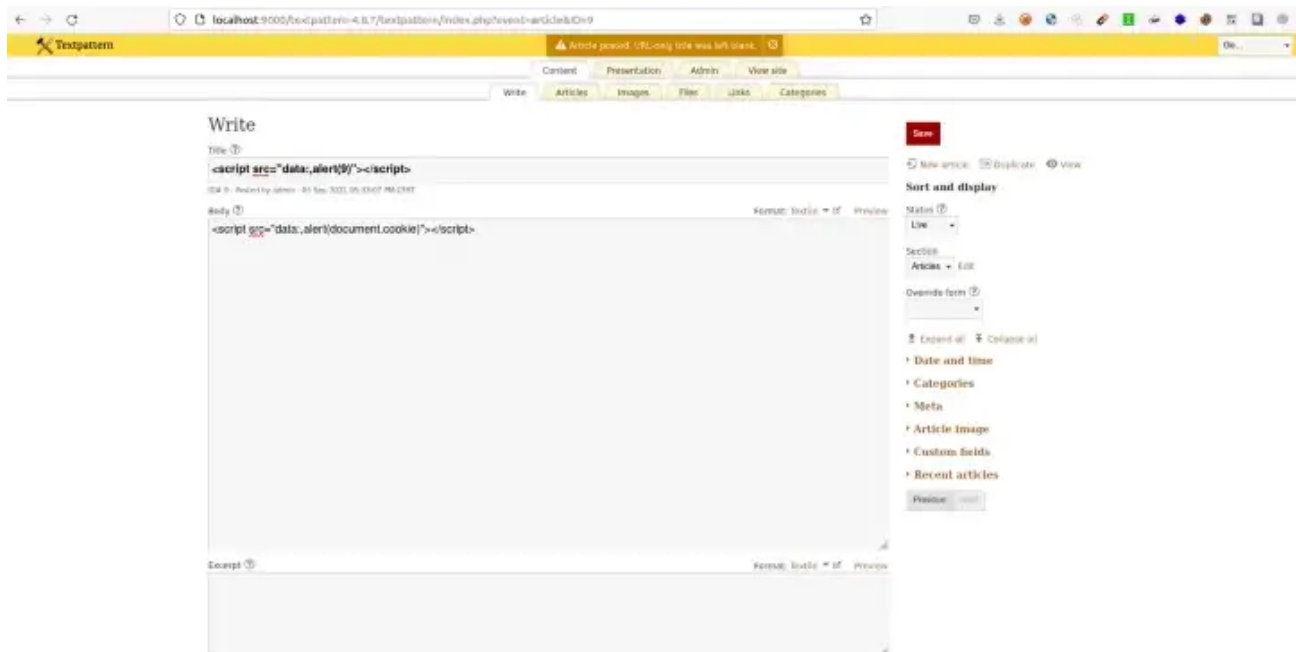
Vendor Homepage: <https://www.textpattern.co>

Software Link: <https://textpattern.com/start>

Version: 4.8.7

Tested on: Ubuntu

Vulnerable Parameters: Body.



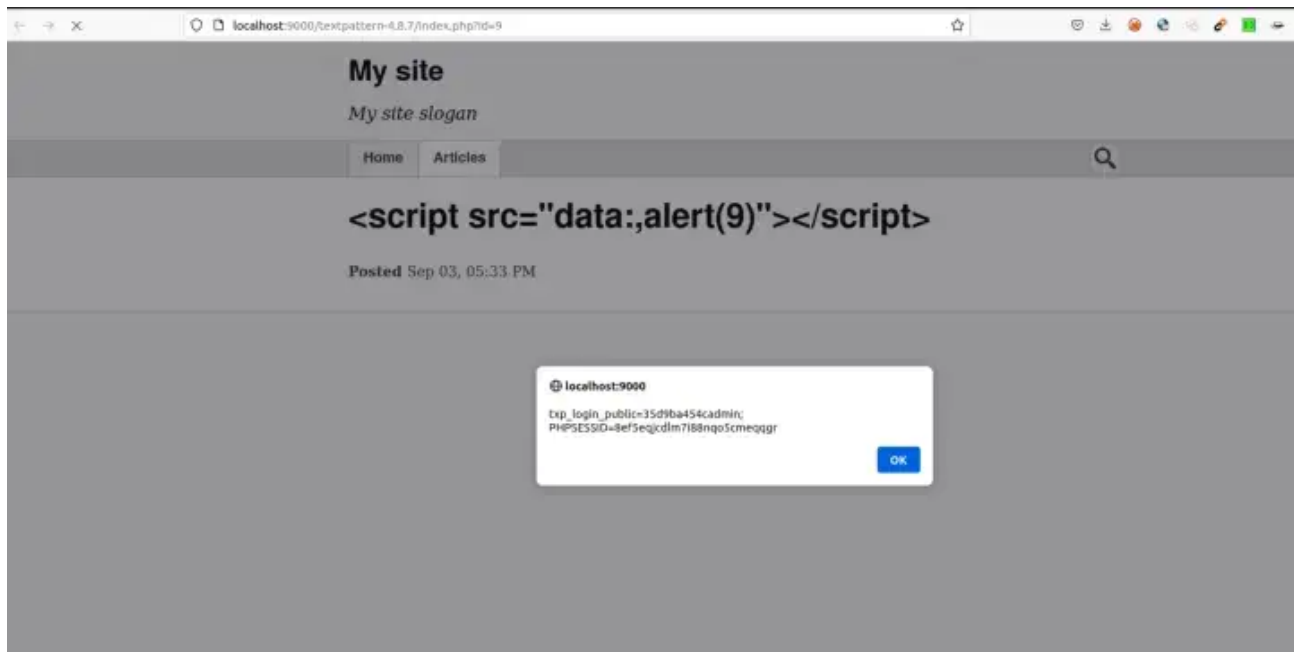
Attack Vector:

This vulnerability can results attacker to inject the HTML src & href attributes payload into the body parameter.

HTML Injection Quick Reference

Annotated concepts and examples for HTML injection (cross-site scripting) tests

[mutantzombie.github.io](https://github.com/mutantzombie)



Steps-To-Reproduce:

1. Login into Textpattern CMS admin panel.
2. Now go to the Content > Write > Body.
3. Now paste the below payload in the URL field.
<script src="data:;alert(document.cookie)"></script>
4. Now click on publish button and click on view button. Boom Boom Boom
5. The HTML payload triggered successfully and give us cookie info with user information.

No bruteforcing, happy with manual testing.

Have a nice day.

Thanks,

Tanmay

Get an email whenever Tanmay Bhattacharjee publishes.

Your email

 Subscribe

By signing up, you will create a Medium account if you don't already have one. Review our [Privacy Policy](#) for more information about our privacy practices.

[About](#) [Help](#) [Terms](#) [Privacy](#)

Get the Medium app