Published in System Weakness

Mayur Parmar Follow
Apr 20, 2021 · 2 min read · Listen

CVE-2020–29247 WonderCMS 3.1.3 — ‘page’ Persistent Cross-Site Scripting

CVE link: https://nvd.nist.gov/vuln/detail/CVE-2020-29247

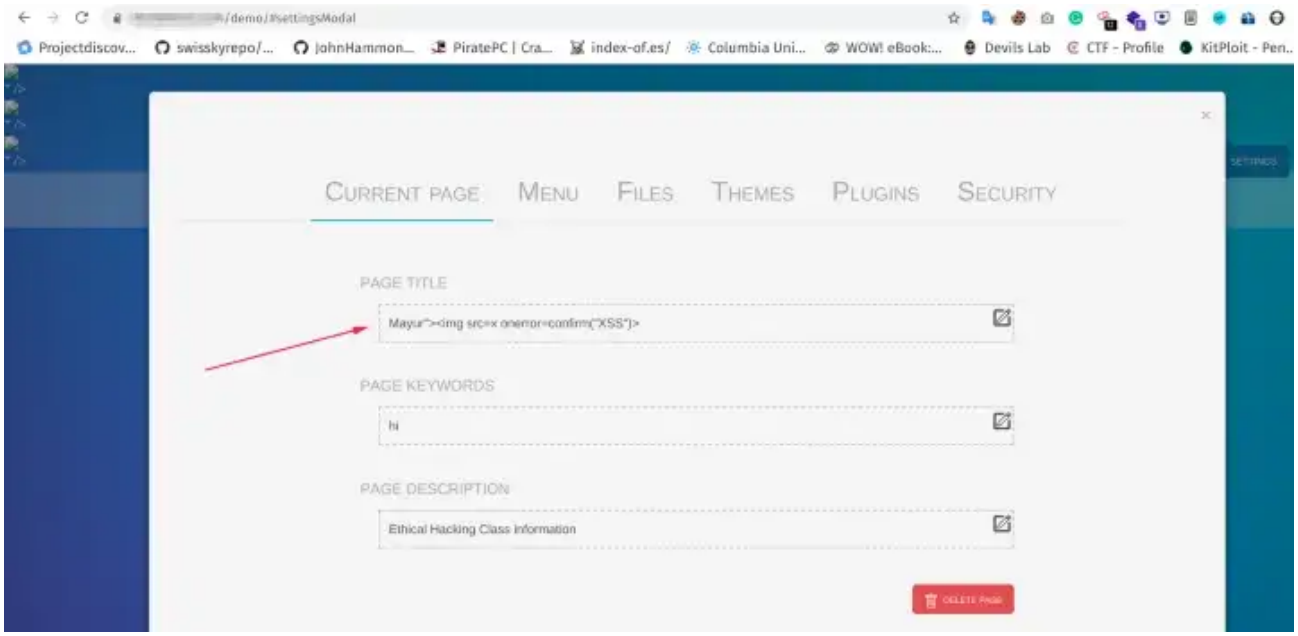
 # Exploit Title: WonderCMS 3.1.3 — ‘page’ Persistent Cross-Site Scripting
 # Date: 20–11–2020
 # Exploit Author: Mayur Parmar
 # Vendor Homepage: https://www.wondercms.com/
 # Version: 3.1.3
 # Tested on: PopOS

Stored Cross-site scripting(XSS):
Stored attacks are those where the injected script is permanently stored on the target servers,
such as in a database, in a message forum, visitor log, comment field, etc.
The victim then retrieves the malicious script from the server when it requests the stored information.
Stored XSS is also sometimes referred to as Persistent XSS.

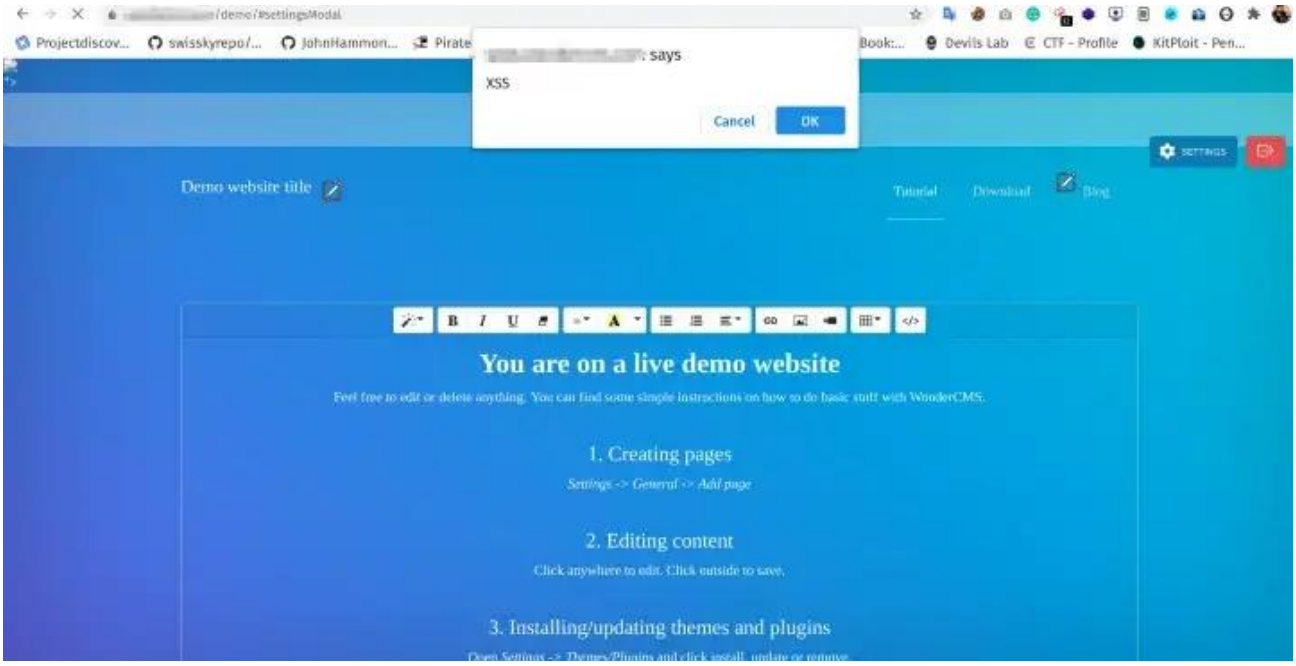
Attack vector:
This vulnerability can results attacker injecting the XSS payload in Page keywords and each time any user will visit the website, the XSS triggers and the attacker can able to steal the cookie according to the crafted payload.

Vulnerable Parameters: Page Title, Page Keywords

Steps-To-Reproduce:
1. Go to the Simple website builder.
2. Put this payload in Page keywords: Mayur”><img src=x onerror=confirm(“XSS”)>



3. Now go to the website and the XSS will be triggered.



Impact:

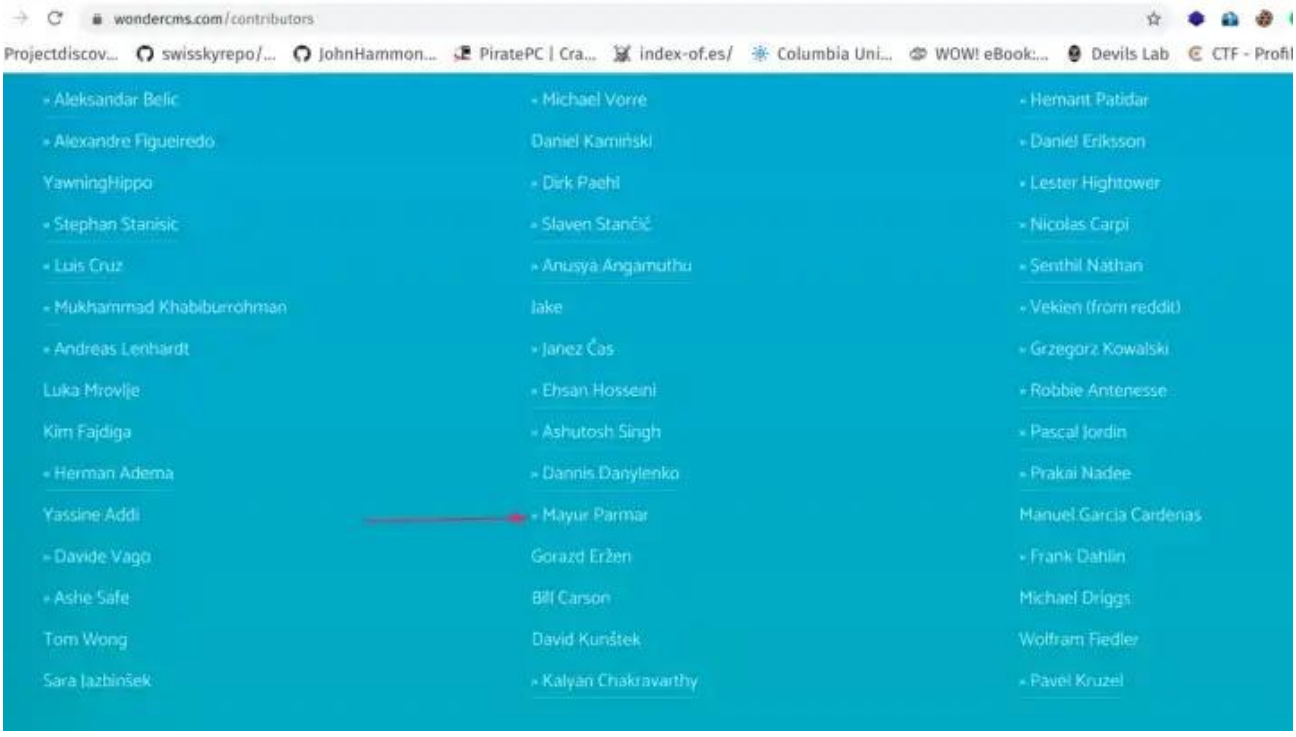
any attacker can inject malicious Javascript code and take over the admin account.

Mitigation:

- **Filter input on arrival.** At the point where user input is received, filter as strictly as possible based on what is expected or valid input.
- **Encode data on output.** At the point where user-controllable data is output in HTTP responses, encode the output to prevent it from being interpreted as active content. Depending on the output context, this might require applying combinations of HTML, URL, JavaScript, and CSS encoding.
- **Use appropriate response headers.** To prevent XSS in HTTP responses that aren't intended to contain any HTML or JavaScript, you can use the `Content-Type` and `X-Content-Type-Options` headers to ensure that browsers interpret the responses in the way you intend.
- **Content Security Policy.** As a last line of defense, you can use Content Security Policy (CSP) to reduce the severity of any XSS vulnerabilities that still occur.

Reward:

For reporting, this vulnerability WonderCMS team appreciated with HallOfFame



Author at: https://systemweakness.com/

Cve Xss Attack Cyber Hacking Zero Day