

Stored Cross Site Scripting vulnerability exists in post content. #1333

Closed SecGus opened this issue on Apr 22, 2020 · 4 comments

SecGus commented on Apr 22, 2020

Summary

A user is able to inject JavaScript into a post via the post creation feature.

Expected Behaviour

The CMS should HTML encode any inputted data so it is reflected back safely to the user.

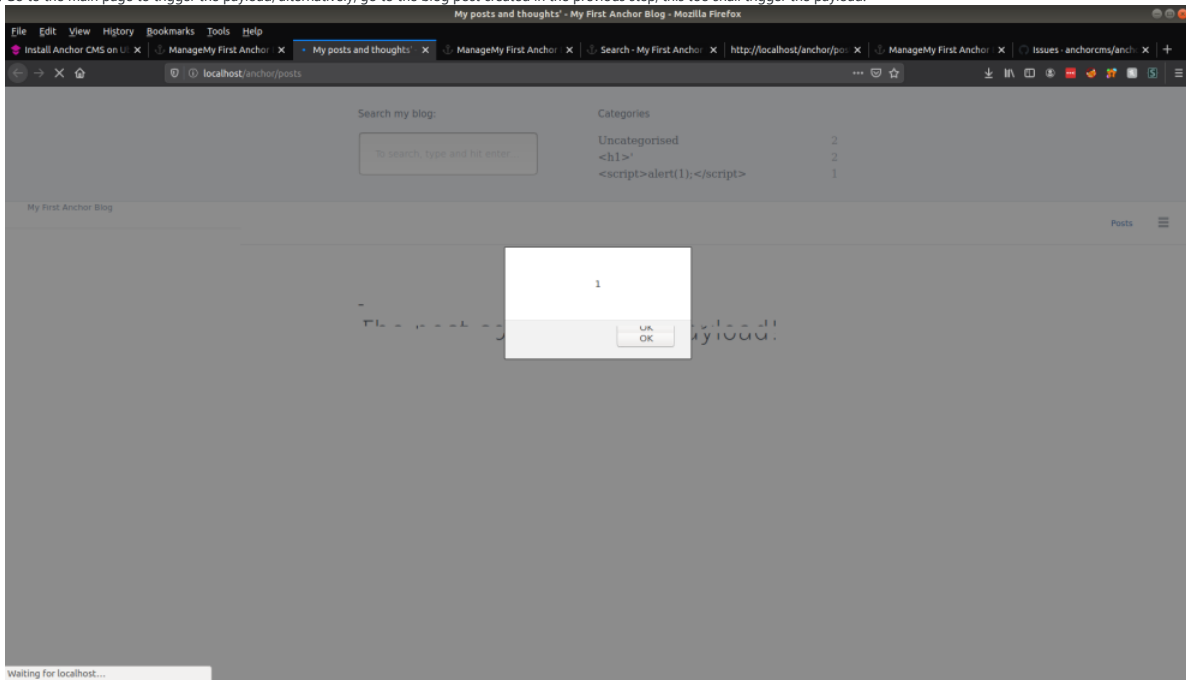
Actual Behaviour

The CMS reflects back the post content without HTML encoding, meaning the client browser renders it as valid HTML / JS on the main page, and on that posts page. This can lead to malicious javascript being executed on anyone who visits the site's browser.

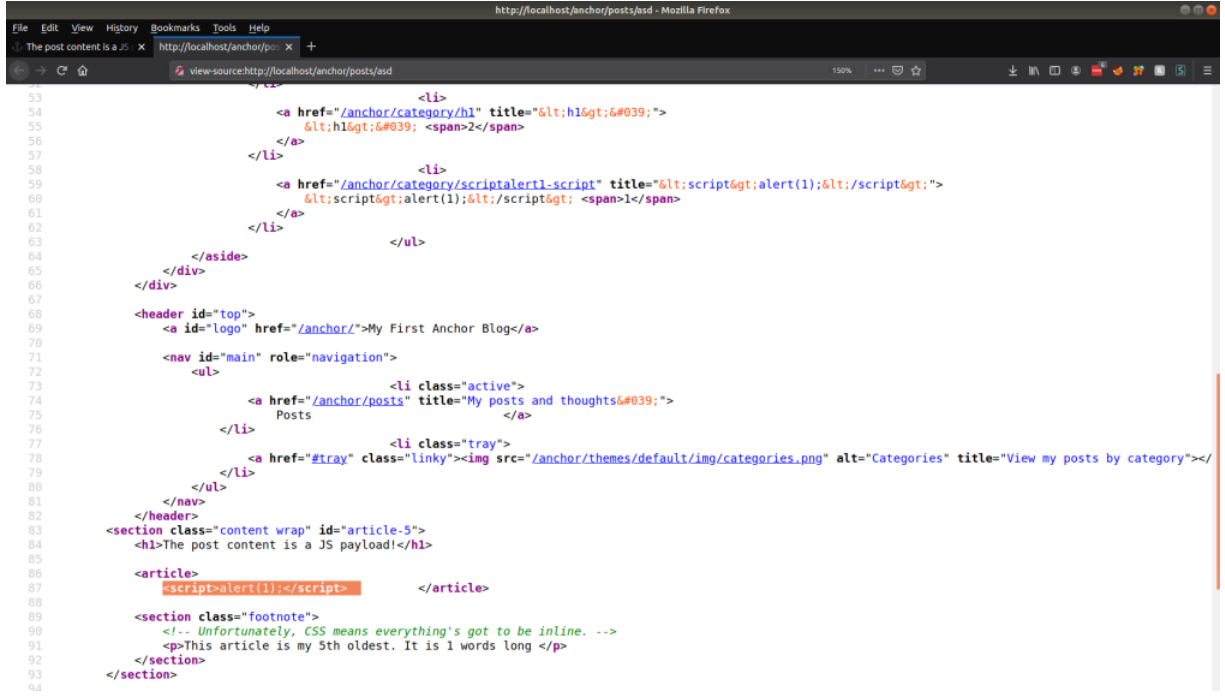
Context details (if applicable)

- Anchor version: 0.12.7
- Server setup: Ubuntu running apache2 and PHP 7.2
- Reproduction:

1. Login to admin panel.
2. Create a blog post where the post title can be anything, and post content is an XSS payload, in my case, I used `<script>alert(1);</script>`.
3. Go to the main page to trigger the payload, alternatively, go to the blog post created in the previous step, this too shall trigger the payload.



As we can see in the blog post source, the title and category are both HTML encoded before being reflected back to the user, although, the post content is not, and our browser renders our JS as valid code.



```
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
```


<a href="/anchor/category/h1" title="<h1>'";><h1>' 2

<a href="/anchor/category/scriptalert1-script" title="<script>alert(1);</script>";><script>alert(1);</script> 1

</aside>
</div>
</div>
<header id="top">
My First Anchor Blog
<nav id="main" role="navigation">

<li class="active">
Posts

<li class="tray">


</nav>
</header>
<section class="content wrap" id="article-5">
<h1>The post content is a JS payload!</h1>
<article>
<script>alert(1);</script>
</article>
<section class="footnote">
<!-- Unfortunately, CSS means everything's got to be inline. -->
<p>This article is my 5th oldest. It is 1 words long </p>
</section>
</section>


 SecGus changed the title ~~Stored Cross Site Scripting Exists in post content~~ Stored Cross Site Scripting vulnerability exists in post content. on Apr 22, 2020

daviddarnes commented on Apr 23, 2020

Member

Duplicate of #1298

 daviddarnes marked this as a duplicate of #1298 on Apr 23, 2020

 daviddarnes closed this as completed on Apr 23, 2020

galaktipus commented on Apr 27, 2020

Any relevant commit for the above issue?

TheBrenny commented on Apr 29, 2020

Member

@galaktipus There's no commit because it was deemed to not be an issue. In the thread it was discussed that AnchorCMS has this as a **feature**, and **not** as a **vulnerability**.

Further, in the [contribution guidelines](#), we request that you [search for your issue](#) to see if it's already been reported before opening a new one. This has obviously not been done. :(

SecGus commented on Apr 29, 2020

Author

Apologies, this was my mistake, I did not realize it was a dupe until I had posted the issue. I do recommend blocking event handlers and script tags, to provide some sort of security, but still allowing HTML customizable content. Maybe add toggleable HTML entity encoding. Without this option, the XSS can be exploited for horizontal privilege escalation.

I understand this was added as a feature, but it can still be used maliciously to some extent, and it is worth thinking about how the end user interacts with your product. Of course it is completely your choice on how you move forward with this.

Thank you for your time, and sorry again for the duplicate issue :)

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

4 participants

