Title: Stored XSS vulnerability in OpenCMS version 17.0

Description:

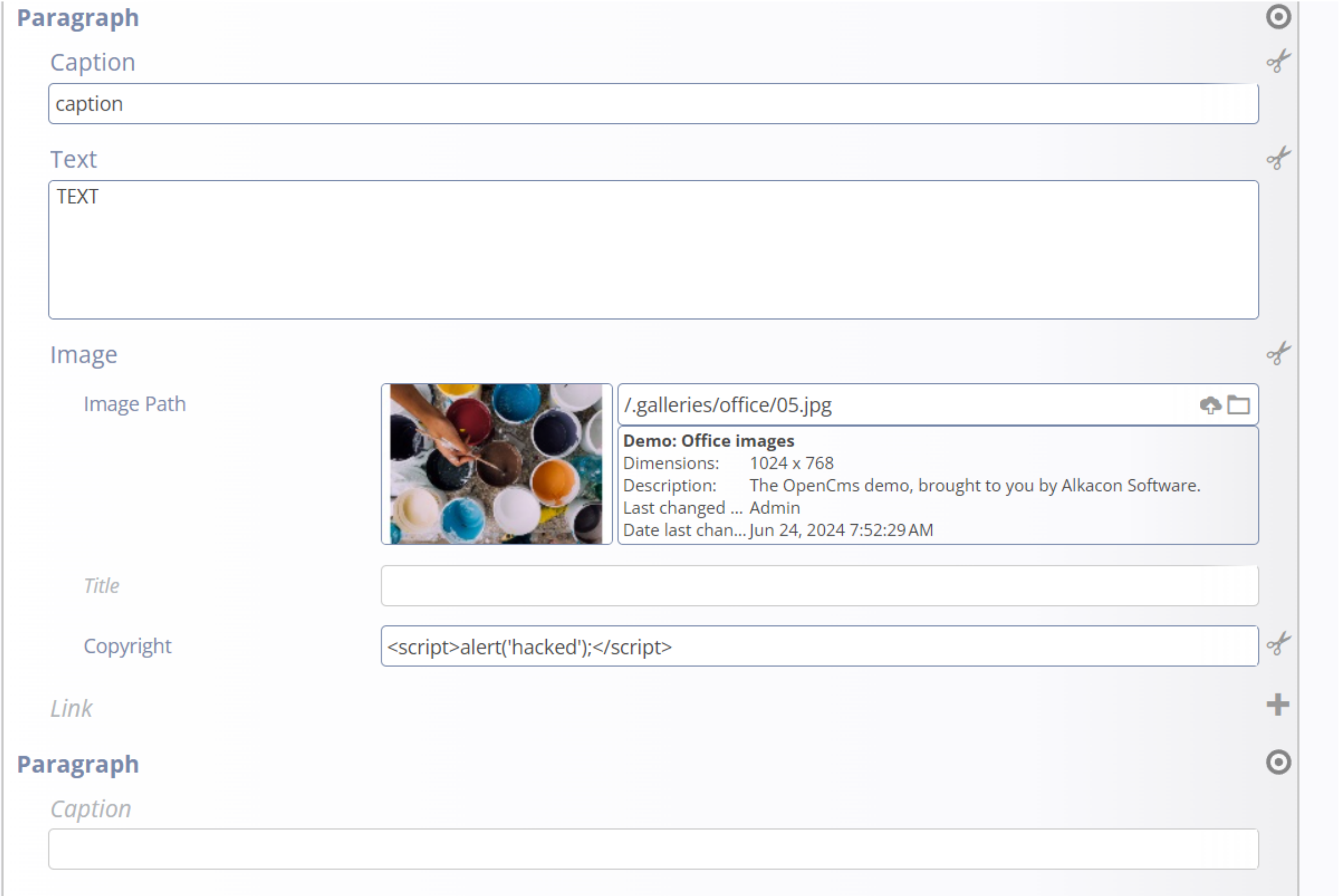
This is a Stored XSS vulnerability in the copyright sub-field in the image field seen when publishing an article.

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 copyright sub-field of the image field write your script like so:



Paragraph

Caption: caption

Text: TEXT

Image

Image Path: /.galleries/office/05.jpg

Demo: Office images
Dimensions: 1024 x 768
Description: The OpenCms demo, brought to you by Alkacon Software.
Last changed ... Admin
Date last chan... Jun 24, 2024 7:52:29 AM

Title:

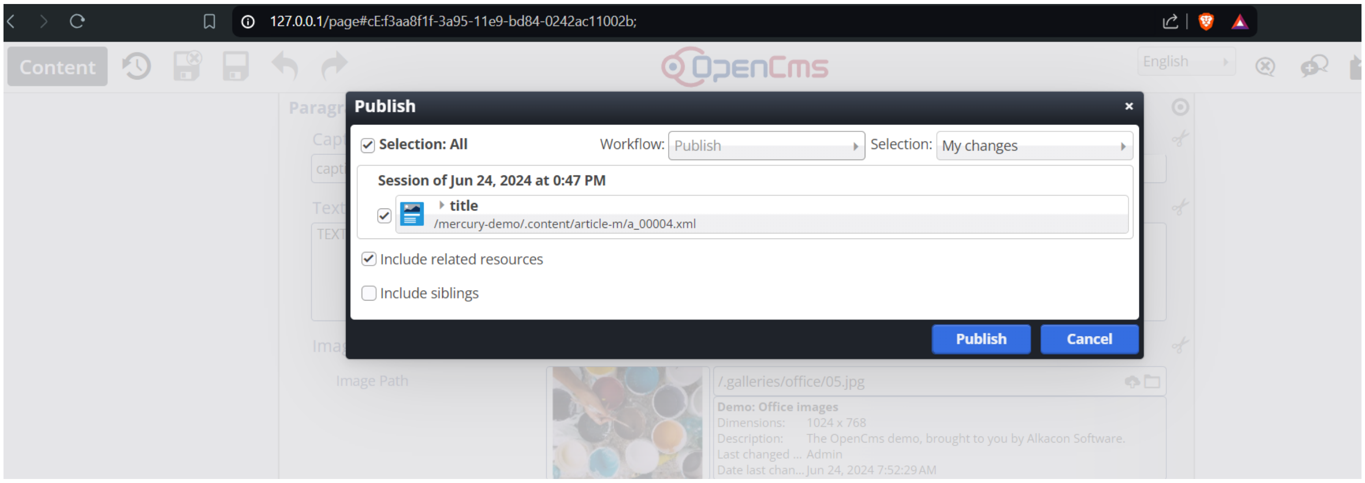
Copyright: <script>alert('hacked');</script>

Link

Paragraph

Caption:

Save and publish your article:



127.0.0.1/page#cE:f3aa8f1f-3a95-11e9-bd84-0242ac11002b;

Publish

☑ **Selection: All** Workflow: Publish Selection: My changes

Session of Jun 24, 2024 at 0:47 PM

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

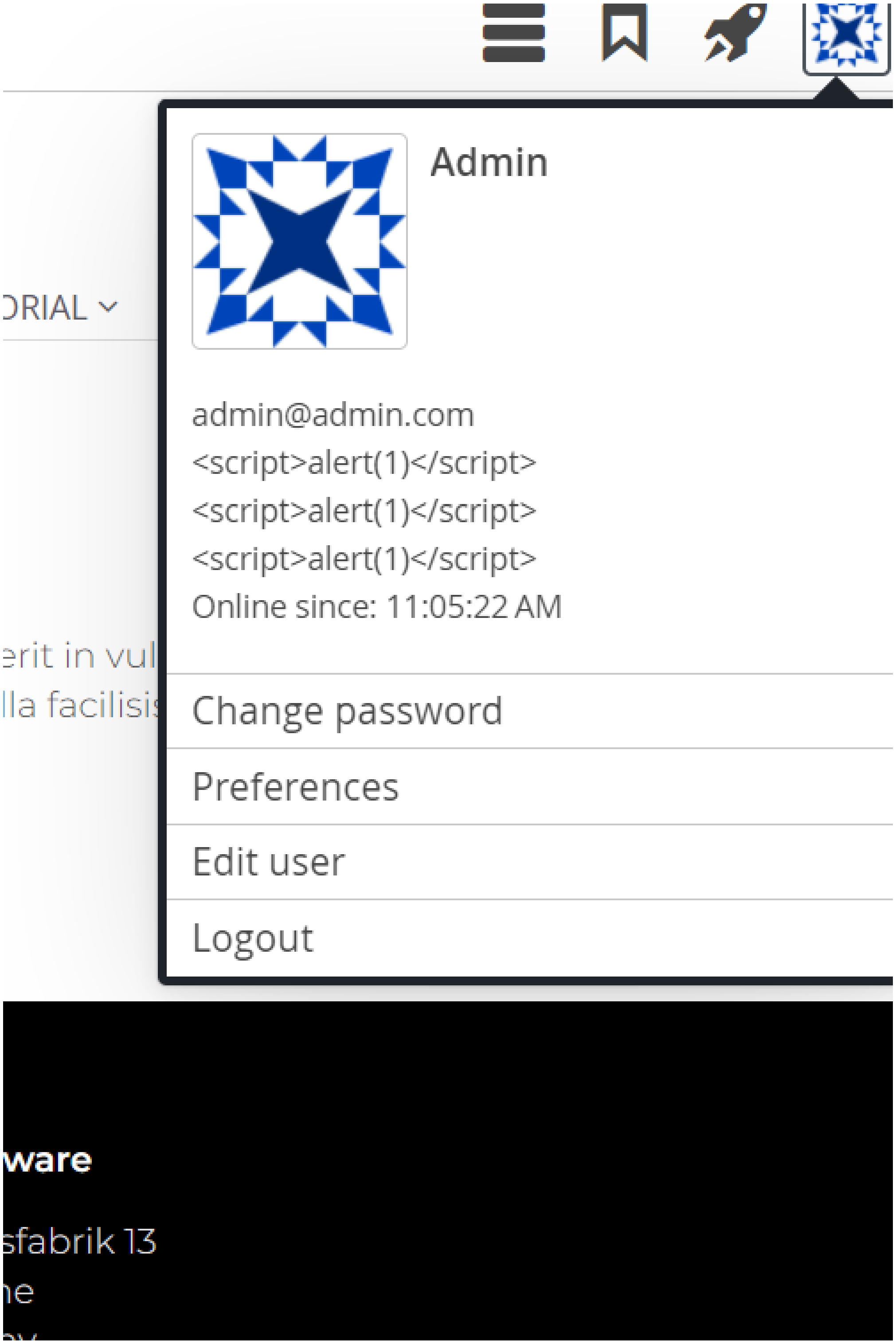
☑ Include related resources

□ Include siblings

Image Path /.galleries/office/05.jpg

Demo: Office images
Dimensions: 1024 x 768
Description: The OpenCms demo, brought to you by Alkacon Software.
Last changed ... Admin
Date last chan... Jun 24, 2024 7:52:29 AM

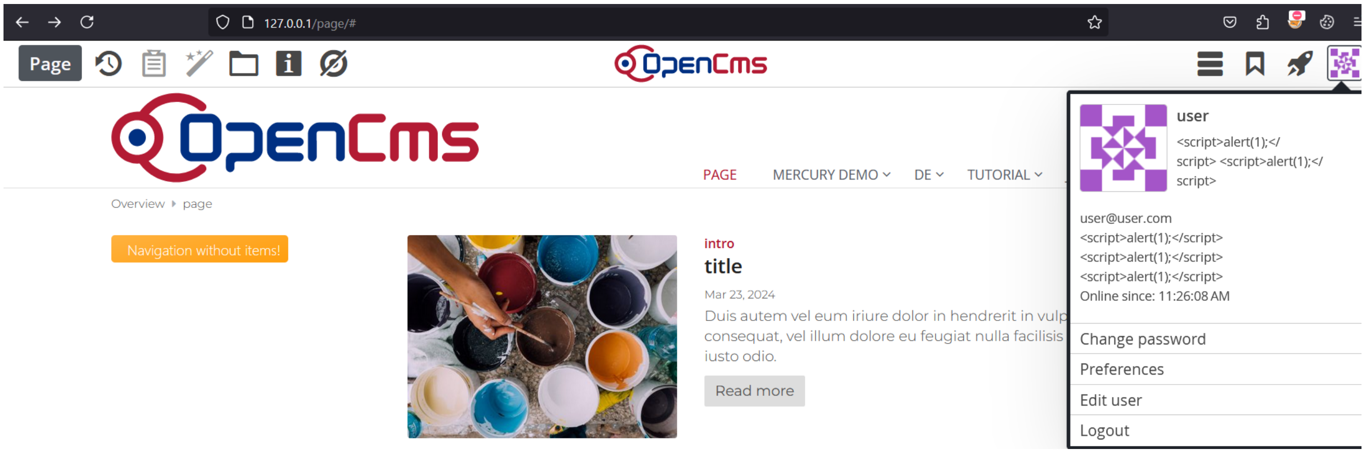
the user who published the article:



Admin

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

The user who clicks on the "read more" button

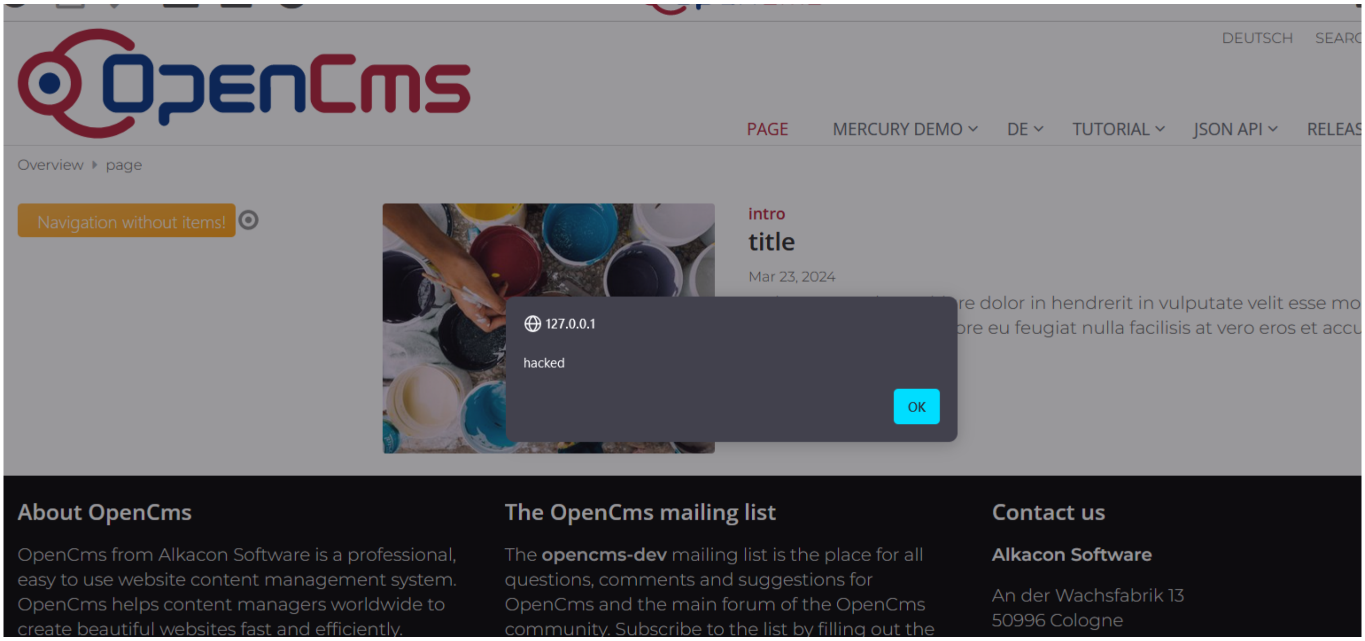


user
<script>alert(1);</
script> <script>alert(1);</
script>

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:



127.0.0.1

hacked

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

About OpenCms

OpenCms from Alkacon Software is a professional, easy to use website content management system. OpenCms helps content managers worldwide to create beautiful websites fast and efficiently.

The OpenCms mailing list

The **opencms-dev** mailing list is the place for all questions, comments and suggestions for OpenCms and the main forum of the OpenCms community. Subscribe to the list by filling out the

Contact us

Alkacon Software

An der Wachsfabrik 13
50996 Cologne

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