

Title: Stored XSS vulnerability in OpenCMS version 17.0

Description:

This is a Stored XSS vulnerability in the title 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 title sub-field of the image field write your script like so:

Content

OpenCms

English

title

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

Article

Author

Text adjustments

Availability

Intro

intro

Title

title

Date

03/23/2024 07:40 PM

Preface

preface

Image

Paragraph

Caption

caption

Text

TEXT

image

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

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

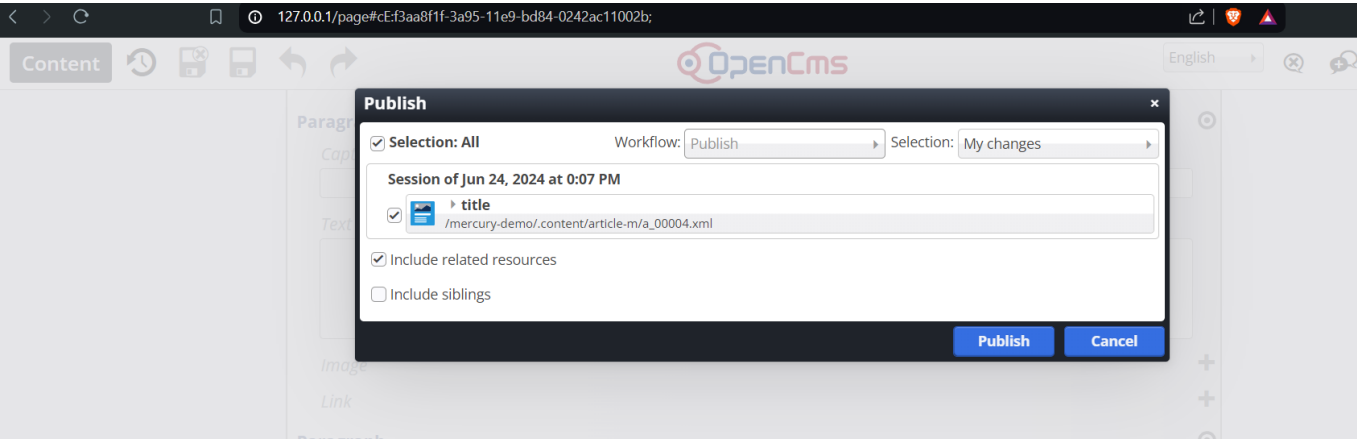
Copyright

CC0 Public Domain / unsplash.com

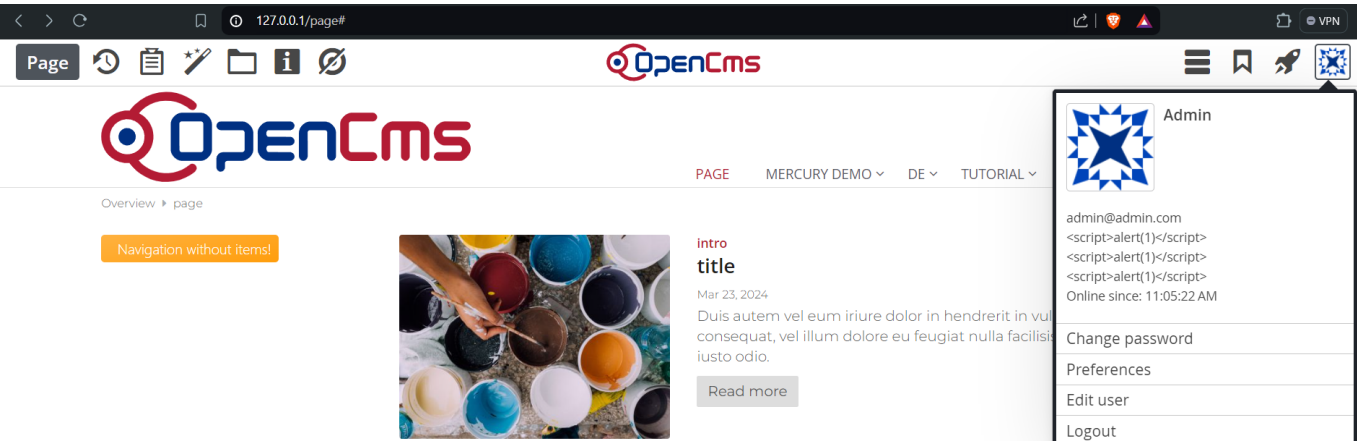
Link

Paragraph

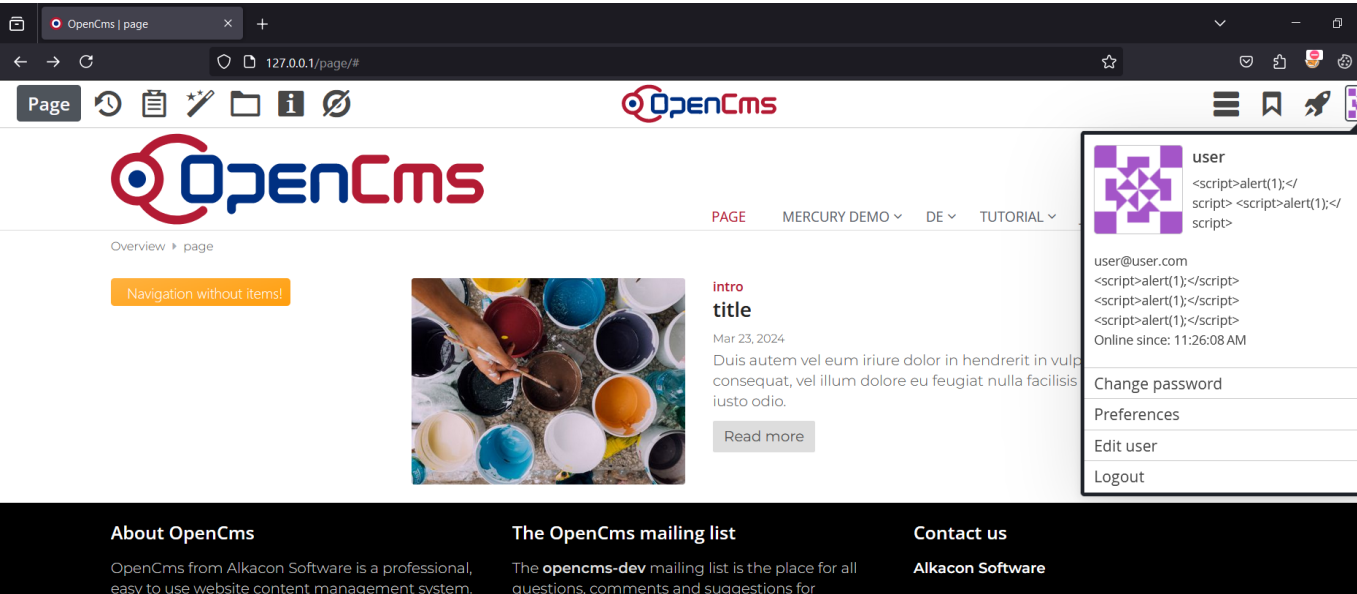
Save and publish the article:



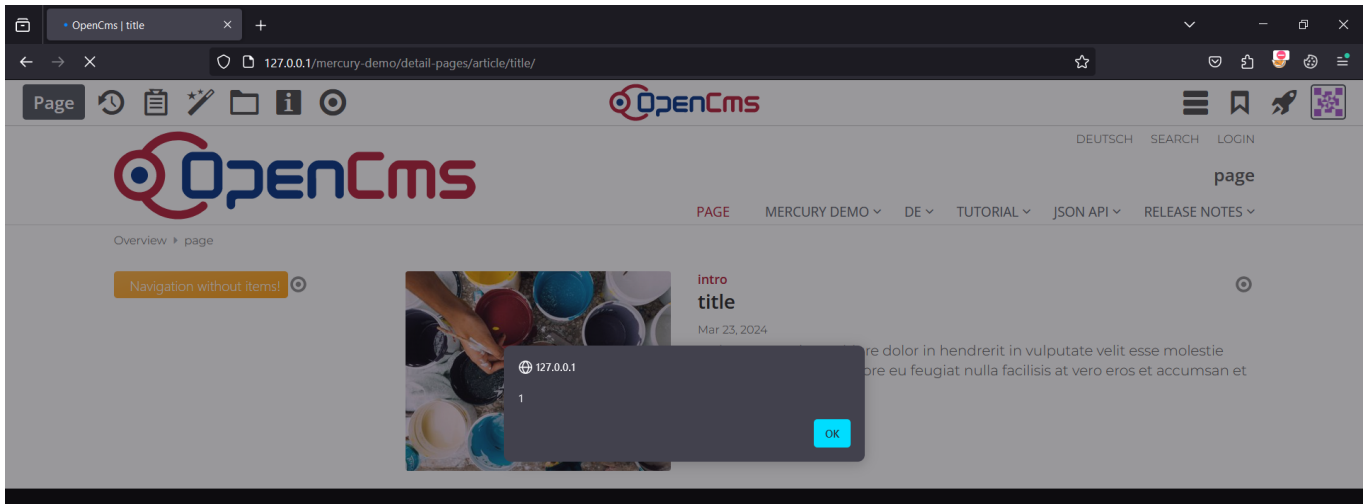
The user to exploits the vulnerability:



The user who clicks on the Read more button



Exploitation Proof:



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>