Type of vulnerability: Persistent XSS.

Affected software: WolfCMS (0.8.3.1).

Description:

Wolf CMS simplifies content management by offering an elegant user interface, flexible templating per page, simple user management, and permissions, as well as the tools necessary for file management.

Type of vulnerability:

Persistent XSS.

URL:

http://www.wolfcms.org/

Vulnerable URL:

http://127.0.0.8/?/admin/page/edit/1

Vulnerable parameter:
Input field name: - page_tag[tags]
Input field id: - page_tags

Vulnerability Description:

Cross-Site Scripting (XSS) attacks are a type of injection, in which malicious scripts are injected into otherwise benign and trusted websites. XSS attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end user. Flaws that allow these attacks to succeed are quite widespread and occur anywhere a web application uses input from a user within the output it generates without validating or encoding it.

Proof of concept: -

Step - 1: Logged in as Admin Role
Step - 2: Select any page (Home Page) locate Metadata put XSS payload “><svg/onload=alert("Provensec")>
Step - 3: It will store the Name as javascript code and it will execute cross-site scripting.

Screenshot attached:

Discovered by:

Provensec

Website:

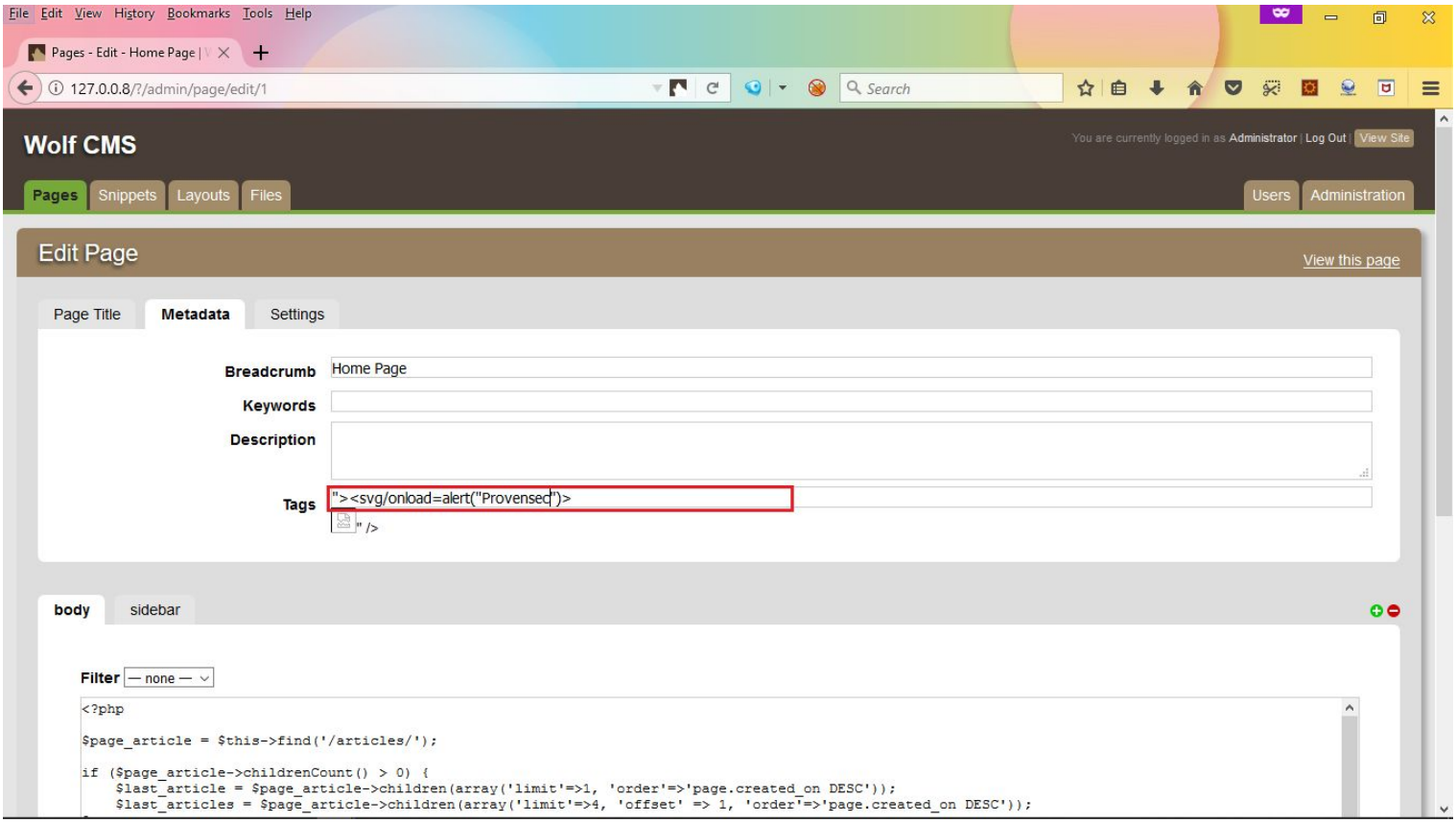
http://www.provensec.com

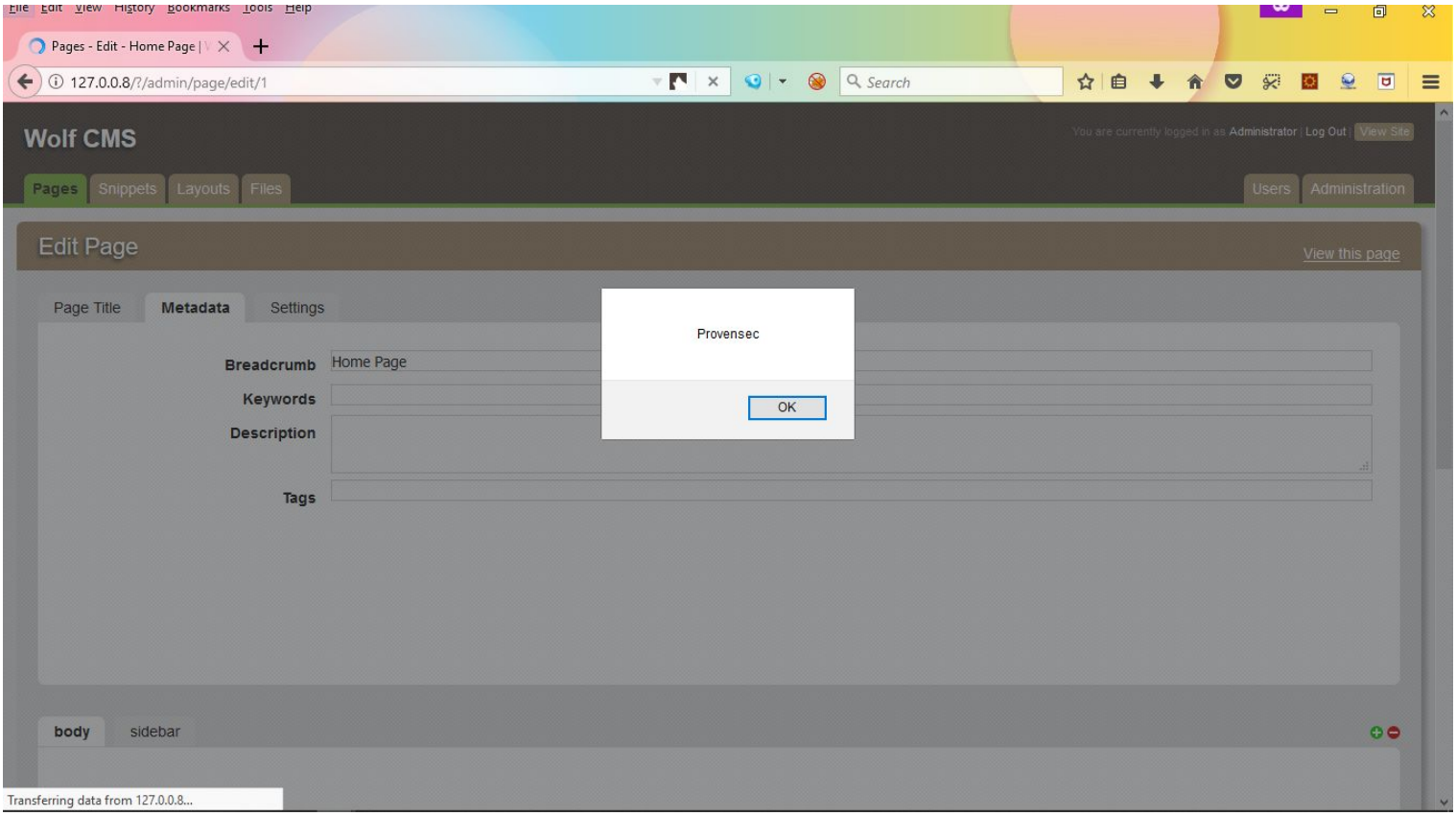
Author:

Subodh Kumar

Reference(s):

https://www.linkedin.com/in/subodh-kumar-8a00b1125/
https://twitter.com/Subodhk62060242
https://github.com/s-kustm




File Edit View History Bookmarks Tools Help
Pages - Edit - Home Page |
127.0.0.8/?/admin/page/edit/1
Search
Wolf CMS
You are currently logged in as Administrator | Log Out | View Site
Pages
Snippets
Layouts
Files
Users
Administration
Edit Page
View this page
Page Title
Metadata
Settings
Breadcrumb
Home Page
Keywords
Description
Tags
Provensec
OK
body
sidebar
Transferring data from 127.0.0.8...