New issue

Jump to bottom

Cross Site Script Vulnerability on "Page" in BlackCAT CMS 1.3.6 #401

Closed r0ck3t1973 opened this issue on Sep 17, 2020 · 2 comments

Assignees	
Labels	security
Milestone	v1.4

r0ck3t1973 commented on Sep 17, 2020 • edited

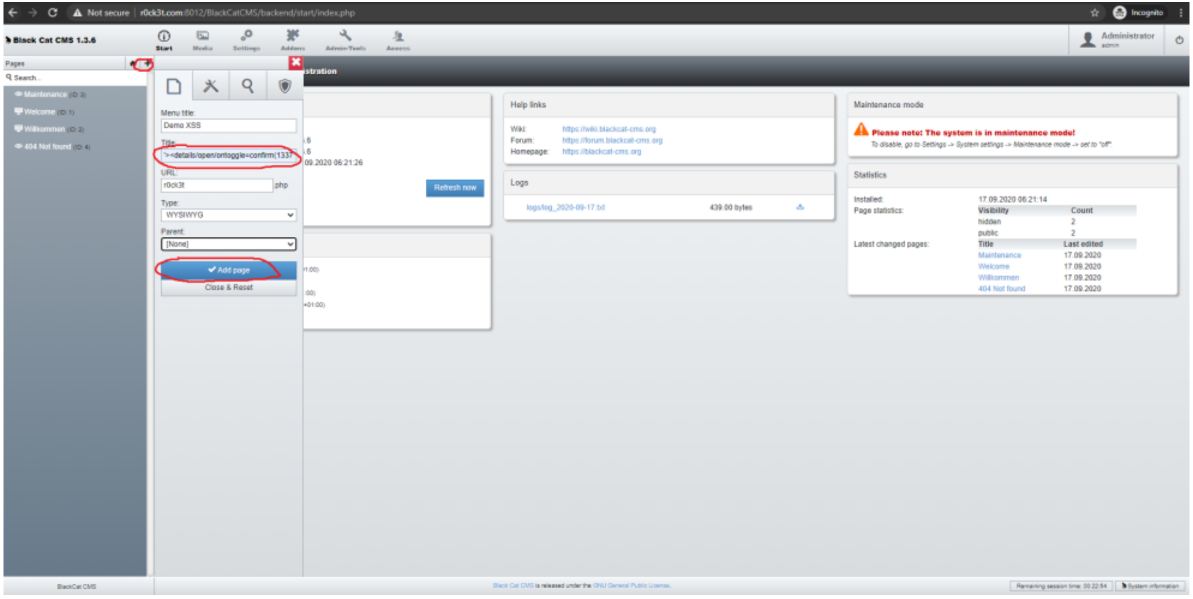
Describe the bug
An authenticated malicious user can take advantage of a Stored XSS vulnerability in the "Add Page" feature in Admin

To Reproduce
Steps to reproduce the behavior:

1. Login into the Admin panel
2. Go to 'BlackCatCMS/backend/start/index.php'
3. Click 'Add Page'
4. Insert Payload in 'Title':
   '><details/open/ontoggle=confirm(1337)>
5. Click 'Add Page'
6. XSS Alert Message

Expected behavior
The removal of script tags is not sufficient to prevent an XSS attack. You must HTML Entity encode any output that is reflected back to the page
Screenshots

1. insert payload



Not secure | r0ck3t.com:8012/BlackCatCMS/backend/start/index.php

Black Cat CMS 1.3.6

Menu title: Demo XSS

Title: '><details/open/ontoggle=confirm(1337

URL: r0ck3t .php

Type: WYSIWYG

Parent: [None]

✔ Add page

Close & Reset

Help links

Wiki: https://wiki.blackcat-cms.org
Forum: https://forum.blackcat-cms.org
Homepage: https://blackcat-cms.org

Logs

logs/log_2020-09-17.txt 439.00 bytes

Maintenance mode

Please note! The system is in maintenance mode!
To disable, go to Settings -> System settings -> Maintenance mode -> set to "off".

Statistics

Installed: 17.09.2020 06:21:14

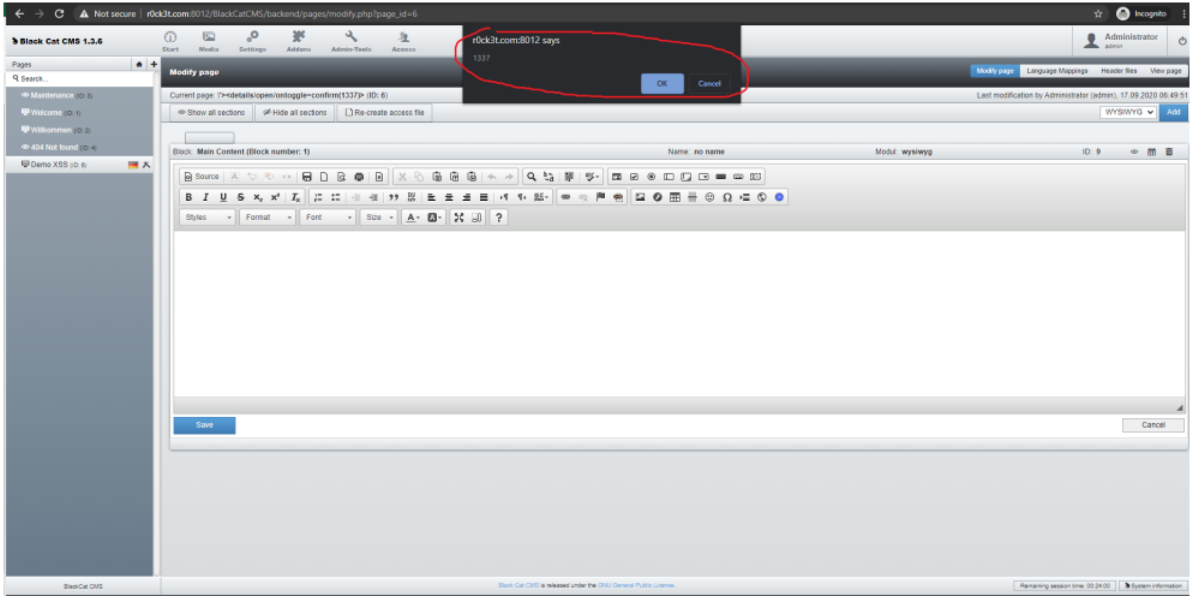
Page statistics:

Visibility	Count
hidden	2
public	2

Latest changed pages:

Title	Last edited
Maintenance	17.09.2020
Welcome	17.09.2020
Willkommen	17.09.2020
404 Not found	17.09.2020

2. xss alert message



r0ck3t.com:8012/BlackCatCMS/backend/pages/modify.php?page_id=6

r0ck3t.com:8012 says

1337

Current page: '/><details/open/ontoggle=confirm(1337)> (ID: 6)

Last modification by Administrator (admin), 17.09.2020 06:49:51

Block: Main Content (Block number: 1) Name: no name Modul: wysiwyg ID: 9

Desktop (please complete the following information):

OS: Windows
Browser: All
Version

webbird self-assigned this on Sep 17, 2020

webbird added the **security** label on Sep 17, 2020

webbird added this to the **v1.4** milestone on Sep 17, 2020

webbird commented on Sep 17, 2020 Contributor

Thank you for reporting this! Will be fixed with upcoming release 1.4.

r0ck3t1973 closed this as completed on Jul 10, 2021

r0ck3t1973 commented on Jul 10, 2021 Author

CVE-2020-25877

webbird reopened this on Jul 12, 2021

webbird pushed a commit that referenced this issue on Sep 24, 2021

`issue #401` 652b4e6

webbird closed this as completed on Sep 24, 2021

Assignees

webbird

Labels

security

Projects

None yet

Milestone

v1.4

Development

No branches or pull requests

2 participants