

New issue

Jump to bottom

Cross Site Script Vulnerability on "Admin-Tools" in BlackCAT CMS 1.3.6 #402

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 "Admin-Tools" feature in Admin

To Reproduce
Steps to reproduce the behavior:

1. Login into the Admin panel
2. Go to 'BlackCatCMS/backend/admintools/index.php'
3. Click Chose:
+/ BlackCat CMS Output Filters: 'BlackCatCMS/backend/admintools/tool.php?tool=blackcatFilter'
+/ Droplets: 'BlackCatCMS/backend/admintools/tool.php?tool=droplets'
4. Insert Payload
'> <details/open/ontoggle=confirm(1337)>
'> < img src=xx onerror=alert(1) >
5. Save
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. BlackCat CMS Output Filters: 'BlackCatCMS/backend/admintools/tool.php?tool=blackcatfilter'

The following table represents the data shown in the 'BlackCat CMS Output Filters' table across the three screenshots.

Provided by (module)	Filename	Description	Enabled	Code
blackcatfilter	obfuscateEmail	Obfuscates eMail addresses	Yes	FILE
blackcatfilter	cmslink	Processes internal page links	Yes	FILE
blackcatfilter	fixDate	fixes dates emitted from old modules	Yes	FILE
blackcatfilter	searchHighlight	Highlights search terms forwarded from search engines	Yes	FILE
blackcatfilter	><-details/open/ontoggle+confirm(1337)>	Demo XSS	Yes	DB

2. Droplets: 'BlackCatCMS/backend/admintools/tool.php?tool=droplets'

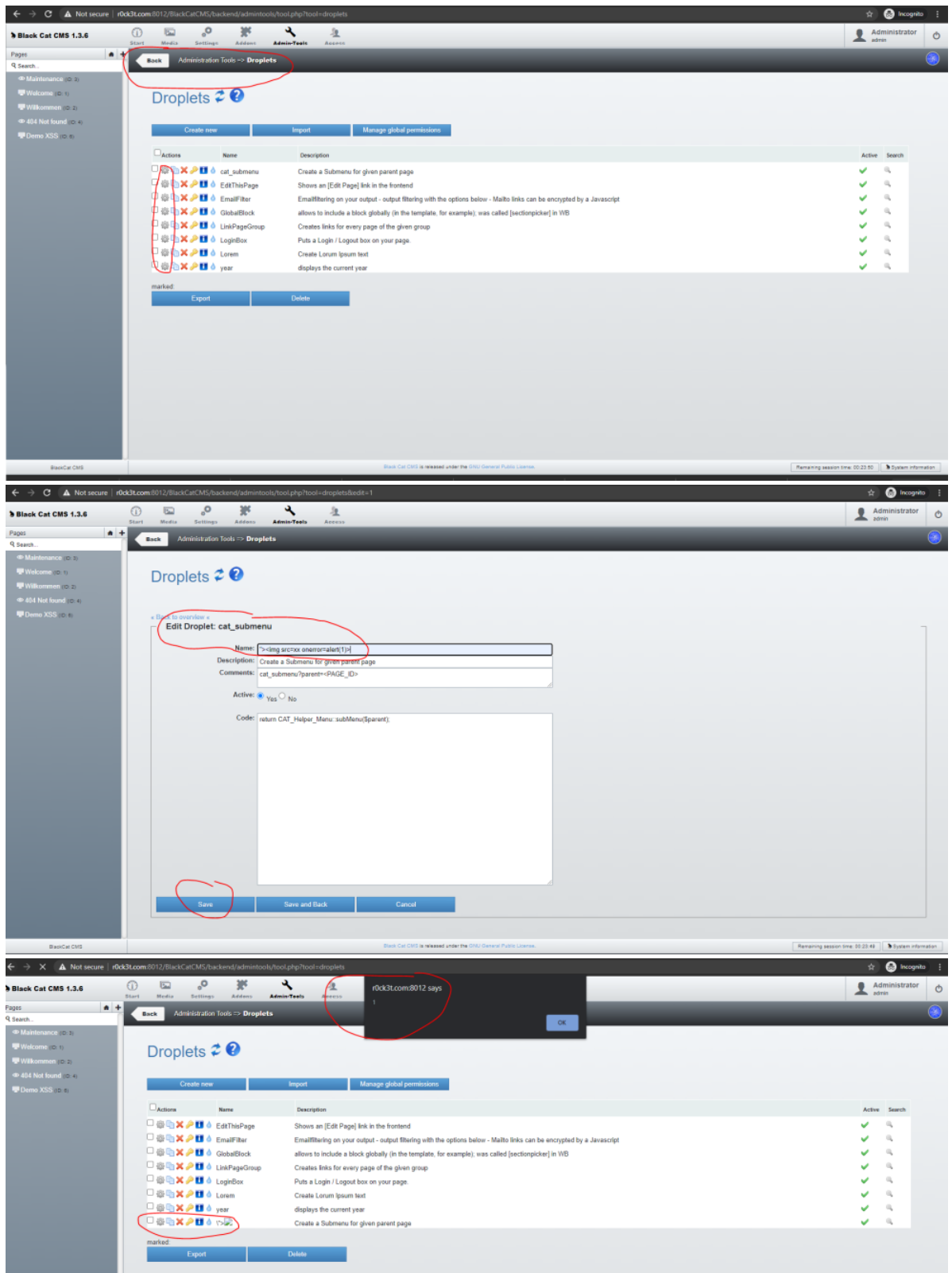
The screenshot shows the BlackCat CMS 1.3.6 interface. The top navigation bar includes 'Start', 'Media', 'Settings', 'Admin-Tools', and 'Access'. The 'Admin-Tools' menu is expanded, showing 'Back', 'Administration Tools -> Droplets', and 'Droplets'. The 'Droplets' page has a 'Create new' button circled in red. Below this is a table of droplets:

Active	Name	Description	Active	Search
<input type="checkbox"/>	cat_submenu	Create a Submenu for given parent page	✓	
<input type="checkbox"/>	EditThisPage	Shows an [Edit Page] link in the frontend	✓	
<input type="checkbox"/>	EmailFilter	EmailFiltering on your output - output filtering with the options below - Mailto links can be encrypted by a Javascript	✓	
<input type="checkbox"/>	GlobalBlock	allows to include a block globally (in the template, for example): was called [sectionpicke] in VIB	✓	
<input type="checkbox"/>	LinkPageGroup	Creates links for every page of the given group	✓	
<input type="checkbox"/>	LoginBox	Puts a Login / Logout box on your page.	✓	
<input type="checkbox"/>	Lorem	Create Lorem Ipsum text	✓	
<input type="checkbox"/>	year	displays the current year	✓	

Below the table are 'Export' and 'Delete' buttons. The 'Edit Droplet' form is also visible, with the 'Name' field containing '><details/openontoggle=confirm(XSS)>' and the 'Code' field containing 'ssaj'. The 'Save' button is circled in red.

r0ck3t.com:8012 says
XSS

OK Cancel



Desktop (please complete the following information):

OS: Windows

Browser: All

Version

webbird self-assigned this on Sep 18, 2020


webbird added this to the v1.4 milestone on Sep 18, 2020

webbird added the security label on Sep 18, 2020

webbird commented on Sep 18, 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-2020-25878](#)

 webbird reopened this on Jul 12, 2021

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

issue [#402](#)

c7da8ed

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

issue [#402](#)

60d145f

 webbird closed this as completed on Sep 24, 2021

  webbird mentioned this issue on Sep 24, 2021

Droplets module needs rewrite #411

 Open

Assignees

 webbird

Labels

security

Projects

None yet

Milestone

v1.4

Development

No branches or pull requests

2 participants