New issue

Jump to bottom

Cross Site Script Vulnerability on "UI Elments" in Codoforum feature V.5.0.2 #4

Closed r0ck3t1973 opened this issue on Sep 15, 2020 · 1 comment

r0ck3t1973 commented on Sep 15, 2020 Owner

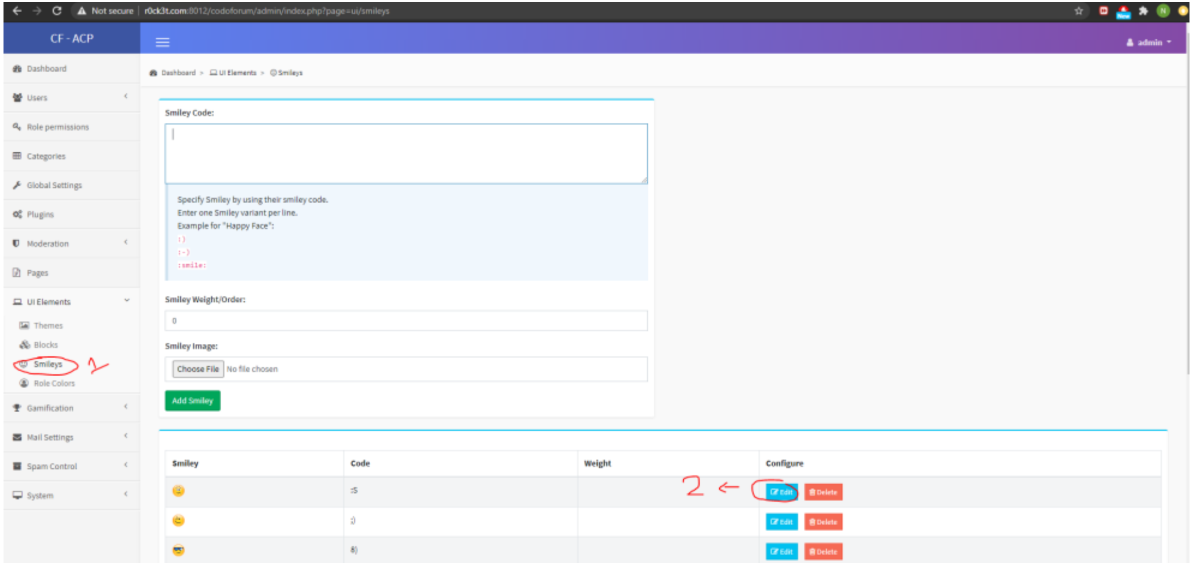
Describe the bug
An authenticated malicious user can take advantage of a Stored XSS vulnerability in the "Smileys" feature.

To Reproduce
Steps to reproduce the behavior:

1. Login into the Admin panel
2. Go to 'codoforum/admin/index.php?page=ui/smileys'
3. Click smileys
4. Choese smileys >> Click Edit
5. Insert Payload 'Smiley Code':
   '><details/open/ontoggle=confirm(1337)>
6. Click Save
7. Go to Page 'codoforum/admin/index.php?page=ui/smileys'
8. 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. Chose smiley



r0ck3t.com:8012/codoforum/admin/index.php?page=ui/smileys

Dashboard > UI Elements > Smileys

Smiley Code:

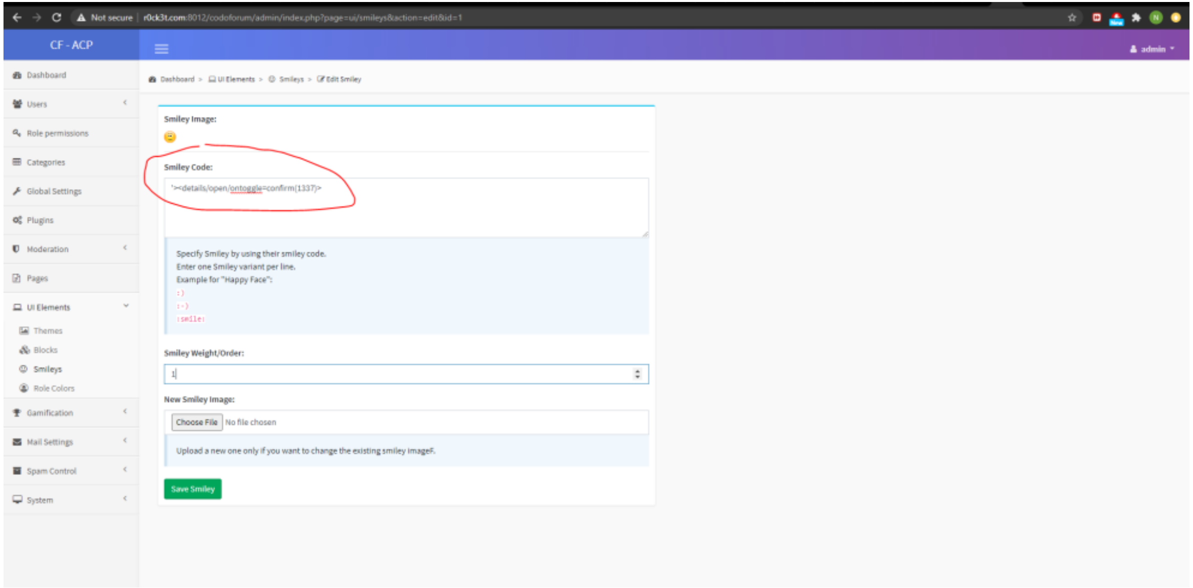
Specify Smiley by using their smiley code.
Enter one Smiley variant per line.
Example for "Happy Face":
:)
:-)
:smile:

Smiley Weight/Order: 0

Smiley Image: No file chosen

Smiley	Code	Weight	Configure
😕	:S		Edit Delete
🙂	:)		Edit Delete
😎	8)		Edit Delete

2. insert payload



r0ck3t.com:8012/codoforum/admin/index.php?page=ui/smileys&action=edit&id=1

Dashboard > UI Elements > Smileys > Edit Smiley

Smiley Image:

Smiley Code: '><details/open/ontoggle=confirm(1337)>

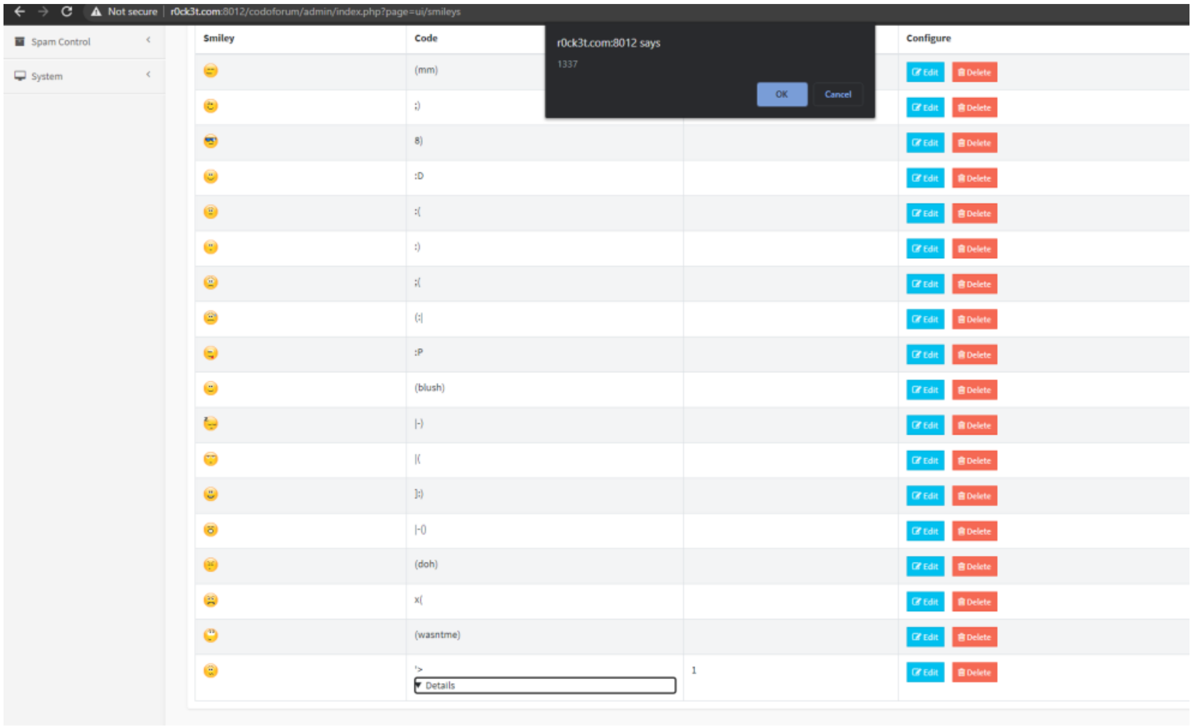
Specify Smiley by using their smiley code.
Enter one Smiley variant per line.
Example for "Happy Face":
:)
:-)
:smile:

Smiley Weight/Order: 1

New Smiley Image: No file chosen

Upload a new one only if you want to change the existing smiley imageF.

3. xss alert mess



r0ck3t.com:8012/codoforum/admin/index.php?page=ui/smileys

r0ck3t.com:8012 says

1337

Smiley	Code		Configure
	(mm)		Edit Delete
	;)		Edit Delete
	8)		Edit Delete
	:D		Edit Delete
	:(		Edit Delete
	:)		Edit Delete
	;(		Edit Delete
	(:|		Edit Delete
	:P		Edit Delete
	(blush)		Edit Delete
	|-)		Edit Delete
	|(		Edit Delete
	]:)		Edit Delete
	|-0		Edit Delete
	(doh)		Edit Delete
	x(		Edit Delete
	(wasntme)		Edit Delete
	'> ▼ Details	1	Edit Delete

Desktop (please complete the following information):

OS: Windows
Browser: All
Version

r0ck3t1973 commented on Jul 10, 2021 Owner Author

CVE-2020-25875

r0ck3t1973 closed this as completed on Jul 10, 2021

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant