dotCMS / **core** Public

Code Issues 331 Pull requests 37 Discussions Actions ...

New issue

Jump to bottom

# Store XSS in dotAdmin/#/c/c_Images on dotcms:21.05.1 #20540

Closed **r0ck3t1973** opened this issue on Jun 14, 2021 · 2 comments

| Labels | Type : Bug |
|---|---|

**r0ck3t1973** commented on Jun 14, 2021

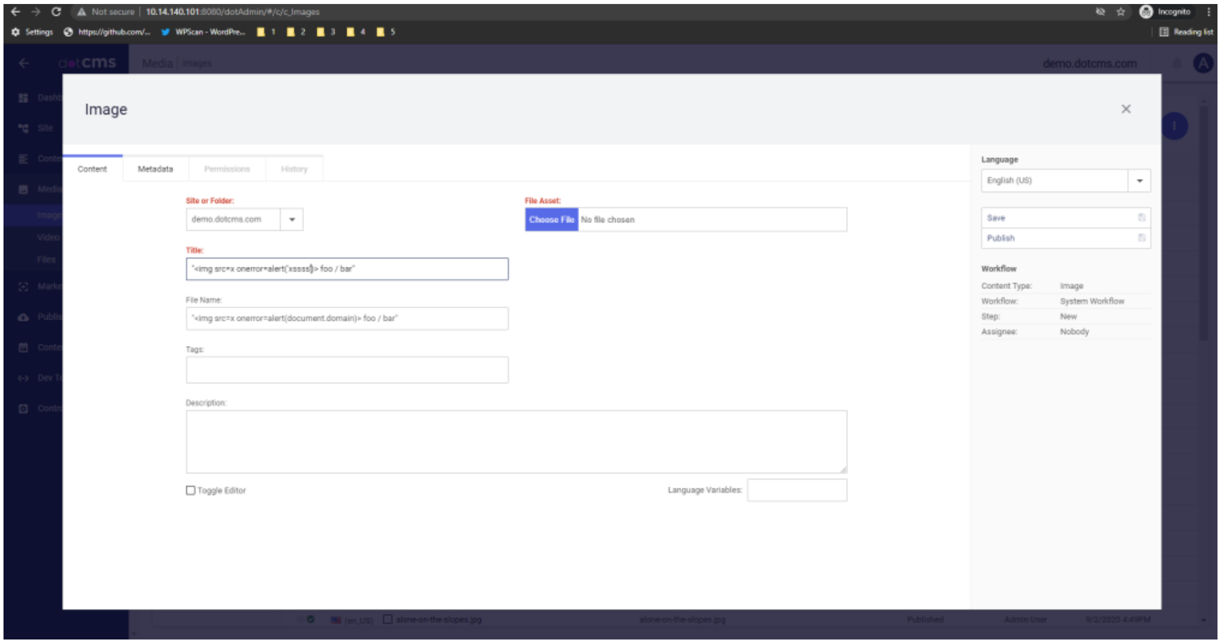
**Describe the bug**
Hi Team
I found small a store xss in dotAdmin/#/c/c_Images
install: Docker: dotcms/dotcms:21.05.1

**To Reproduce**

1. Login Admin panel
2. Go to 'dotAdmin/#/c/c_Images'
3. Click on 'Add new content'
4. Parameter: 'Title' and 'Filename"
5. Insert Payload Store XSS: " foo / bar"
6. Click 'Choose File' and BOOM XSS
7. Save and refersh store XSS

**impact**
Commonly include transmitting private data, like cookies or other session information, to the attacker, redirecting the victim to web content controlled by the attacker, or performing other malicious operations on the user's machine under the guise of the vulnerable site.

Screenshots



Not secure | 10.14.140.101:8080/dotAdmin/#/c/c_Images

Image

Content | Metadata | Permissions | History

Site or Folder: demo.dotcms.com

File Asset: Choose File No file chosen

Title: "<img src=x onerror=alert('xssss')> foo / bar"

File Name: "<img src=x onerror=alert(document.domain)> foo / bar"

Tags:

Description:

□ Toggle Editor

Language Variables:

Language: English (US)

Save

Publish

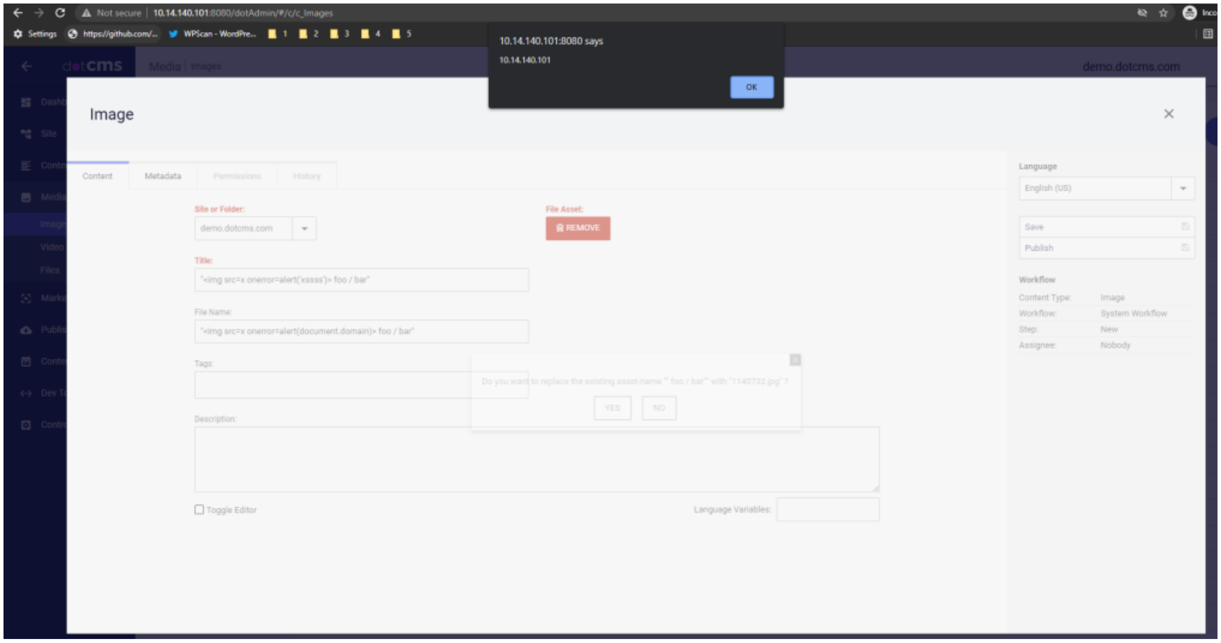
Workflow

Content Type: Image

Workflow: System Workflow

Step: New

Assignee: Nobody



Not secure | 10.14.140.101:8080/dotAdmin/#/c/c_Images

10.14.140.101:8080 says

10.14.140.101

OK

Image

Site or Folder: demo.dotcms.com

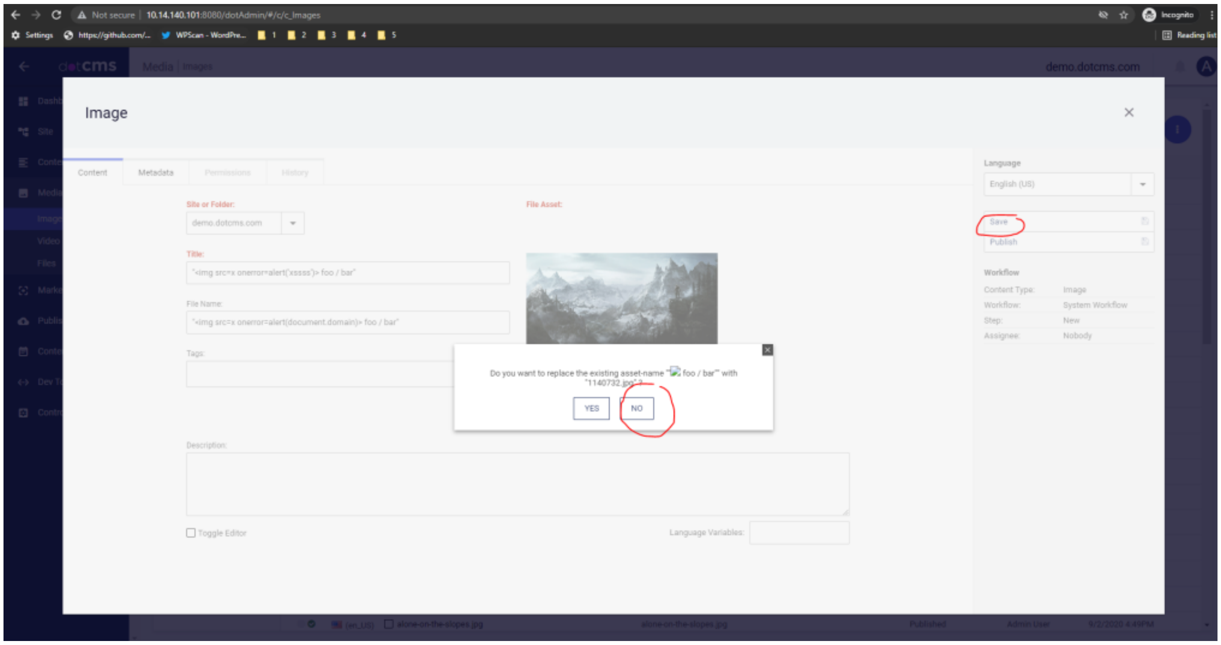
File Asset: REMOVE

Title: "<img src=x onerror=alert('xssss')> foo / bar"

File Name: "<img src=x onerror=alert(document.domain)> foo / bar"

Do you want to replace the existing asset-name " foo / bar"" with "1140732.jpg" ?

YES NO



Not secure | 10.14.140.101:8080/dotAdmin/#/c/c_Images

Image

Site or Folder: demo.dotcms.com

File Asset:

Title: "<img src=x onerror=alert('xssss')> foo / bar"

File Name: "<img src=x onerror=alert(document.domain)> foo / bar"

Do you want to replace the existing asset-name " foo / bar"" with "1140732.jpg" ?

YES [✓ NO]

[✓ Save]

Publish

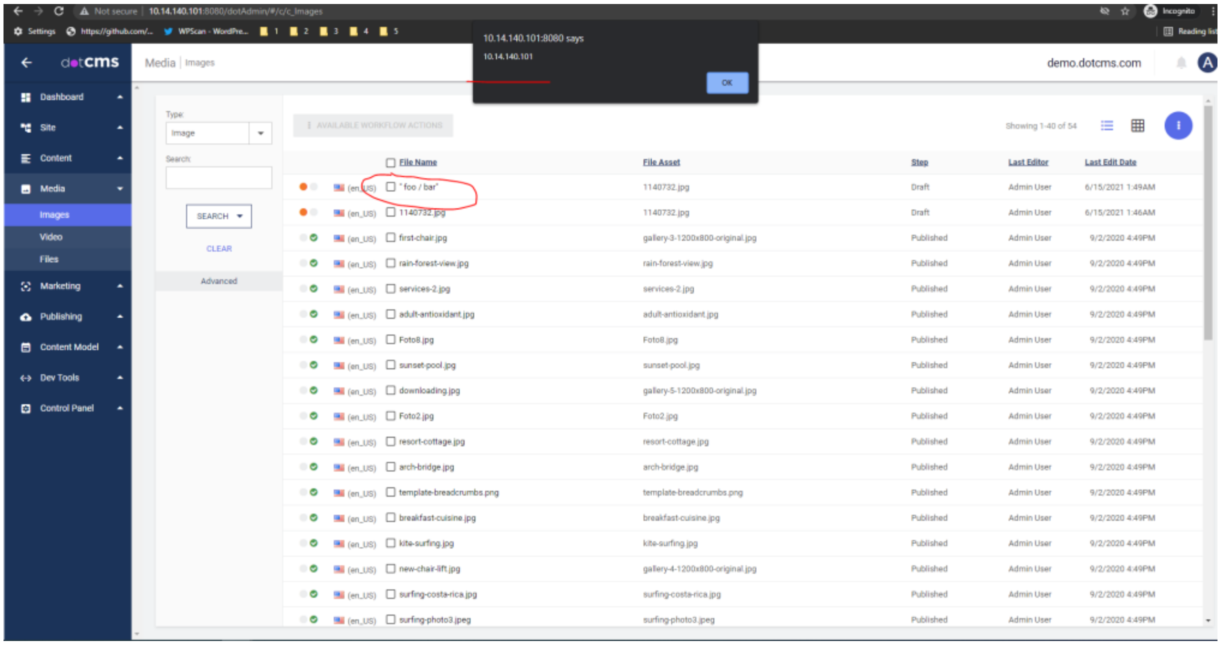
Workflow

Content Type: Image

Workflow: System Workflow

Step: New

Assignee: Nobody



10.14.140.101:8080/dotAdmin/#/c/c_Images

10.14.140.101:8080 says

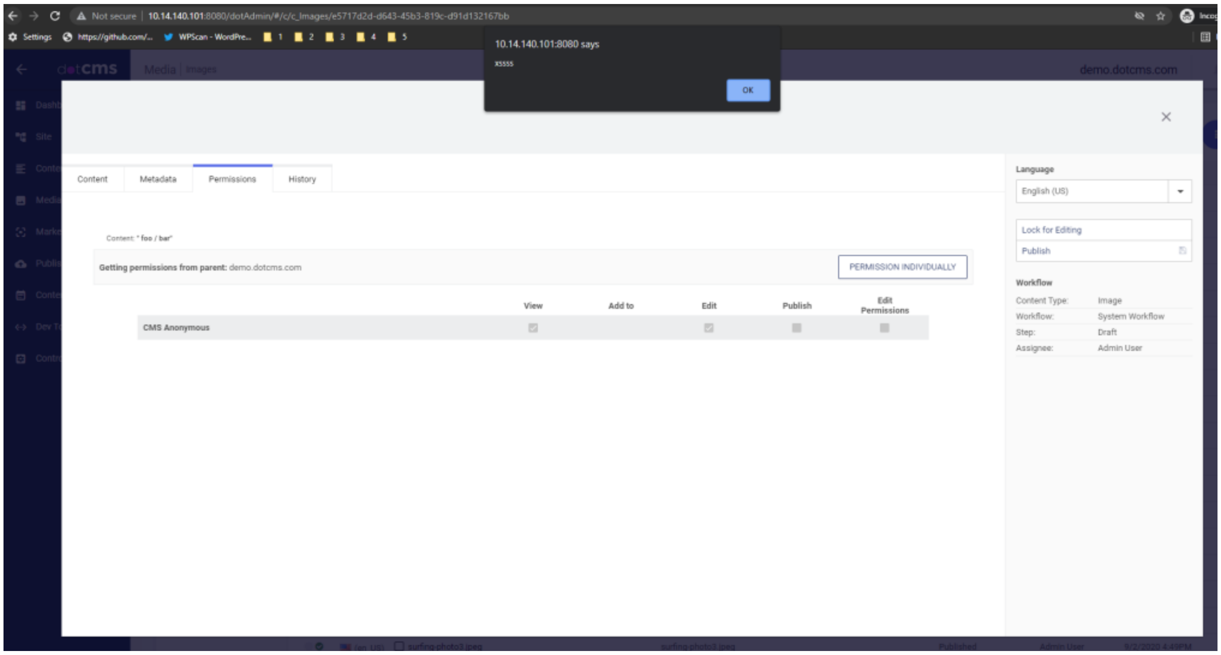
10.14.140.101

Type: Image

Search:

Showing 1-40 of 54

| | | File Name | File Asset | Step | Last Editor | Last Edit Date |
|---|---|---|---|---|---|---|
| ● | (en_US) | □ " foo / bar" | 1140732.jpg | Draft | Admin User | 6/15/2021 1:49AM |
| ● | (en_US) | □ 1140732.jpg | 1140732.jpg | Draft | Admin User | 6/15/2021 1:46AM |
| ✓ | (en_US) | □ first-chair.jpg | gallery-3-1200x800-original.jpg | Published | Admin User | 9/2/2020 4:49PM |
| ✓ | (en_US) | □ rain-forest-view.jpg | rain-forest-view.jpg | Published | Admin User | 9/2/2020 4:49PM |
| ✓ | (en_US) | □ services-2.jpg | services-2.jpg | Published | Admin User | 9/2/2020 4:49PM |
| ✓ | (en_US) | □ adult-antioxidant.jpg | adult-antioxidant.jpg | Published | Admin User | 9/2/2020 4:49PM |
| ✓ | (en_US) | □ Foto8.jpg | Foto8.jpg | Published | Admin User | 9/2/2020 4:49PM |
| ✓ | (en_US) | □ sunset-pool.jpg | sunset-pool.jpg | Published | Admin User | 9/2/2020 4:49PM |
| ✓ | (en_US) | □ downloading.jpg | gallery-5-1200x800-original.jpg | Published | Admin User | 9/2/2020 4:49PM |
| ✓ | (en_US) | □ Foto2.jpg | Foto2.jpg | Published | Admin User | 9/2/2020 4:49PM |
| ✓ | (en_US) | □ resort-cottage.jpg | resort-cottage.jpg | Published | Admin User | 9/2/2020 4:49PM |
| ✓ | (en_US) | □ arch-bridge.jpg | arch-bridge.jpg | Published | Admin User | 9/2/2020 4:49PM |
| ✓ | (en_US) | □ template-breadcrumbs.png | template-breadcrumbs.png | Published | Admin User | 9/2/2020 4:49PM |
| ✓ | (en_US) | □ breakfast-cuisine.jpg | breakfast-cuisine.jpg | Published | Admin User | 9/2/2020 4:49PM |
| ✓ | (en_US) | □ kite-surfing.jpg | kite-surfing.jpg | Published | Admin User | 9/2/2020 4:49PM |
| ✓ | (en_US) | □ new-chair-lift.jpg | gallery-4-1200x800-original.jpg | Published | Admin User | 9/2/2020 4:49PM |
| ✓ | (en_US) | □ surfing-costa-rica.jpg | surfing-costa-rica.jpg | Published | Admin User | 9/2/2020 4:49PM |
| ✓ | (en_US) | □ surfing-photo3.jpeg | surfing-photo3.jpeg | Published | Admin User | 9/2/2020 4:49PM |



10.14.140.101:8080/dotAdmin/#/c/c_Images/e5717d2d-d643-45b3-819c-d91d132167bb

10.14.140.101:8080 says

x5555

Content: " foo / bar"

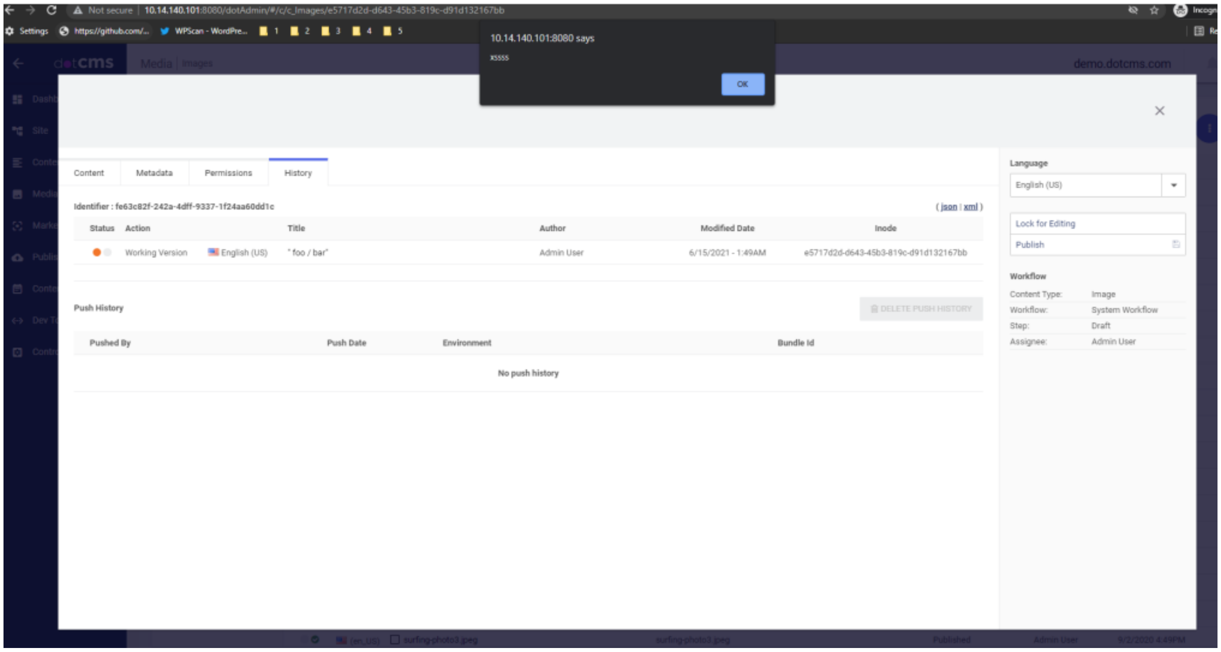
**Getting permissions from parent:** demo.dotcms.com

| | View | Add to | Edit | Publish | Edit Permissions |
|---|---|---|---|---|---|
| CMS Anonymous | ☑ | | ☑ | □ | □ |

Language: English (US)

Workflow

Content Type: Image
Workflow: System Workflow
Step: Draft
Assignee: Admin User



10.14.140.101:8080/dotAdmin/#/c/c_Images/e5717d2d-d643-45b3-819c-d91d132167bb

10.14.140.101:8080 says

xssss

Identifier : fe63c82f-242a-4dff-9337-1f24aa60dd1c ( json | xml )

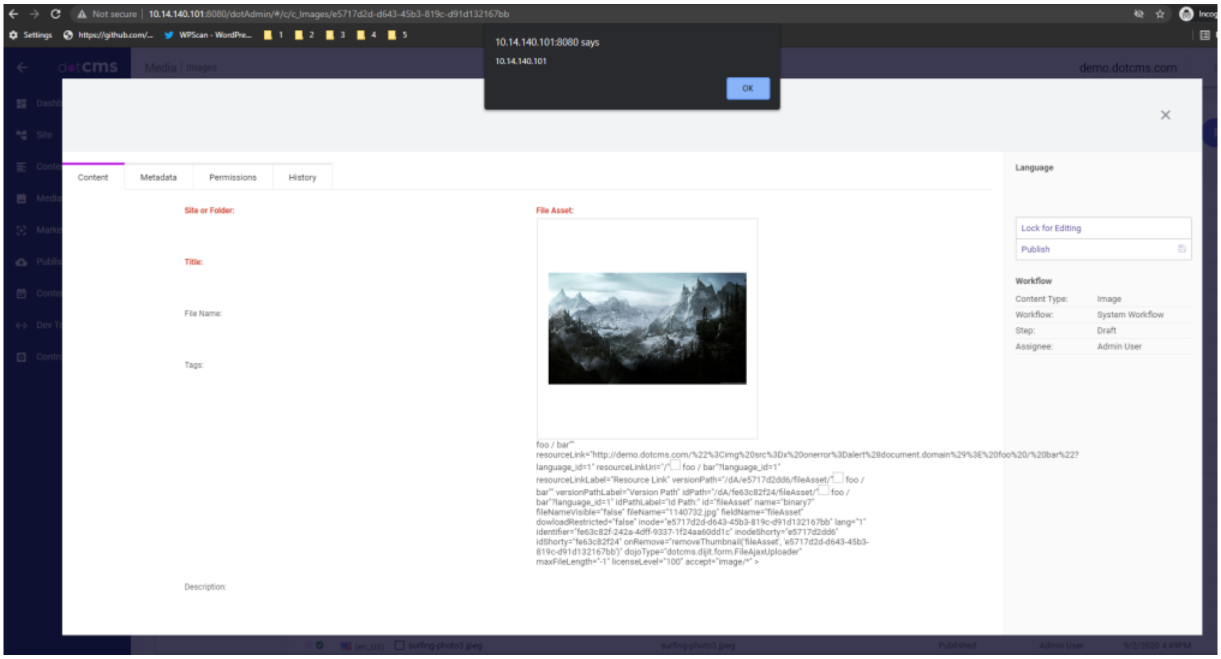
| Status | Action | Title | Author | Modified Date | Inode |
|---|---|---|---|---|---|
| ● | Working Version English (US) | " foo / bar" | Admin User | 6/15/2021 - 1:49AM | e5717d2d-d643-45b3-819c-d91d132167bb |

Push History

| Pushed By | Push Date | Environment | Bundle Id |
|---|---|---|---|
| No push history | | | |

Workflow

| | |
|---|---|
| Content Type: | Image |
| Workflow: | System Workflow |
| Step: | Draft |
| Assignee: | Admin User |



10.14.140.101:8080/dotAdmin/#/c/c_Images/e5717d2d-d643-45b3-819c-d91d132167bb

10.14.140.101:8080 says

10.14.140.101

```
foo / bar""
resourceLink="http://demo.dotcms.com/%22%3Cimg%20src%3Dx%20onerror%3Dalert%28document.domain%29%3E%20foo%20/%20bar%22?
language_id=1" resourceLinkUri="/"□ foo / bar"?language_id=1"
resourceLinkLabel="Resource Link" versionPath="/dA/e5717d2dd6/fileAsset/"□ foo /
bar"" versionPathLabel="Version Path" idPath="/dA/fe63c82f24/fileAsset/"□ foo /
bar"?language_id=1" idPathLabel="Id Path:" id="fileAsset" name="binary7"
fileNameVisible="false" fileName="1140732.jpg" fieldName="fileAsset"
dowloadRestricted="false" inode="e5717d2d-d643-45b3-819c-d91d132167bb" lang="1"
identifier="fe63c82f-242a-4dff-9337-1f24aa60dd1c" inodeShorty="e5717d2dd6"
idShorty="fe63c82f24" onRemove="removeThumbnail('fileAsset', 'e5717d2d-d643-45b3-
819c-d91d132167bb')" dojoType="dotcms.dijit.form.FileAjaxUploader"
maxFileLength="-1" licenseLevel="100" accept="image/*" >
```

Workflow

| | |
|---|---|
| Content Type: | Image |
| Workflow: | System Workflow |
| Step: | Draft |
| Assignee: | Admin User |

Desktop (please complete the following information):

- OS: Win 10
- Browser Chrome: Version 91.0.4472.77 (Official Build) (64-bit)

**r0ck3t1973** added the Type : Bug label on Jun 14, 2021

**wezell** commented on Jun 15, 2021 Contributor

This is a known issue with some of the older admin screens and takes administrative access to exploit. Additionally, dotCMS does not allow http-referers from outside of the known list of sites that it serves, which prevents XSS vulnerabilities like these from being exploitable in the wild.

https://dotcms.com/security/SI-16

**wezell** closed this as completed on Jun 15, 2021

**r0ck3t1973** commented on Jul 10, 2021 Author

CVE-2021-35358

Assignees

No one assigned

Labels

Type : Bug

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants