eddy8 / LightCMS Public

Code Issues Pull requests Discussions Actions Projects ···

New issue

Jump to bottom

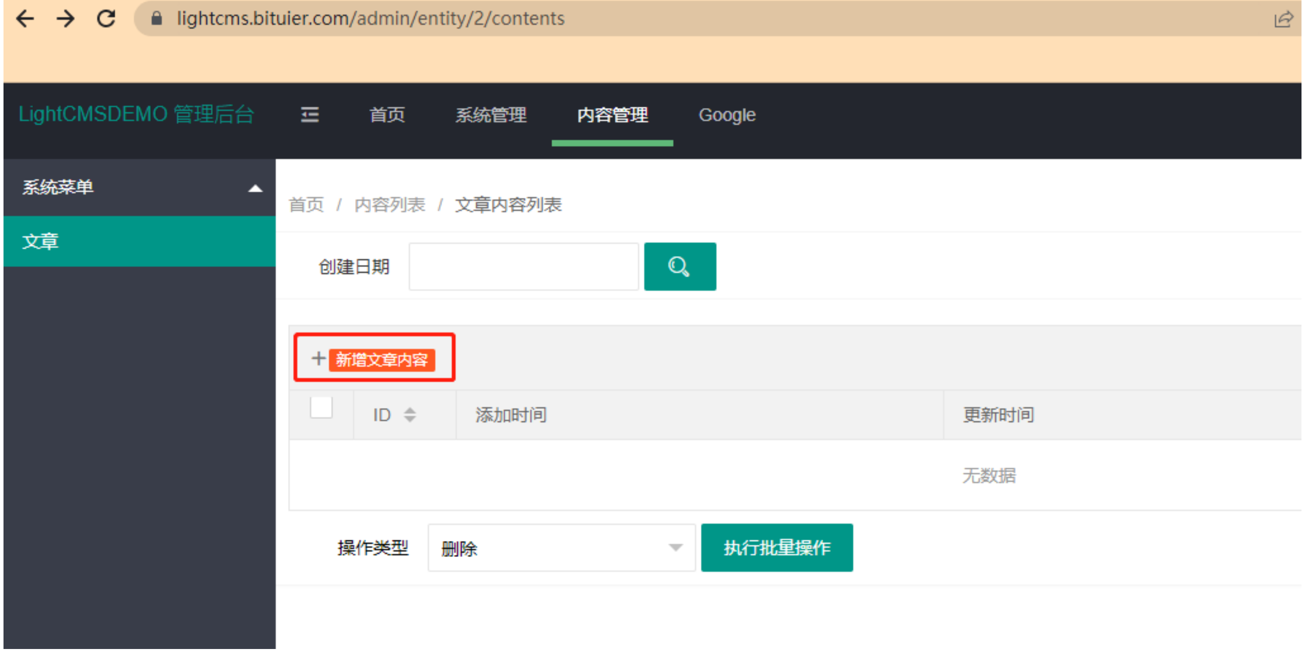
A stored cross-site scripting (XSS) vulnerability exists in LightCMS "contents" field #30

Closed SKdft opened this issue on Jun 6 · 2 comments

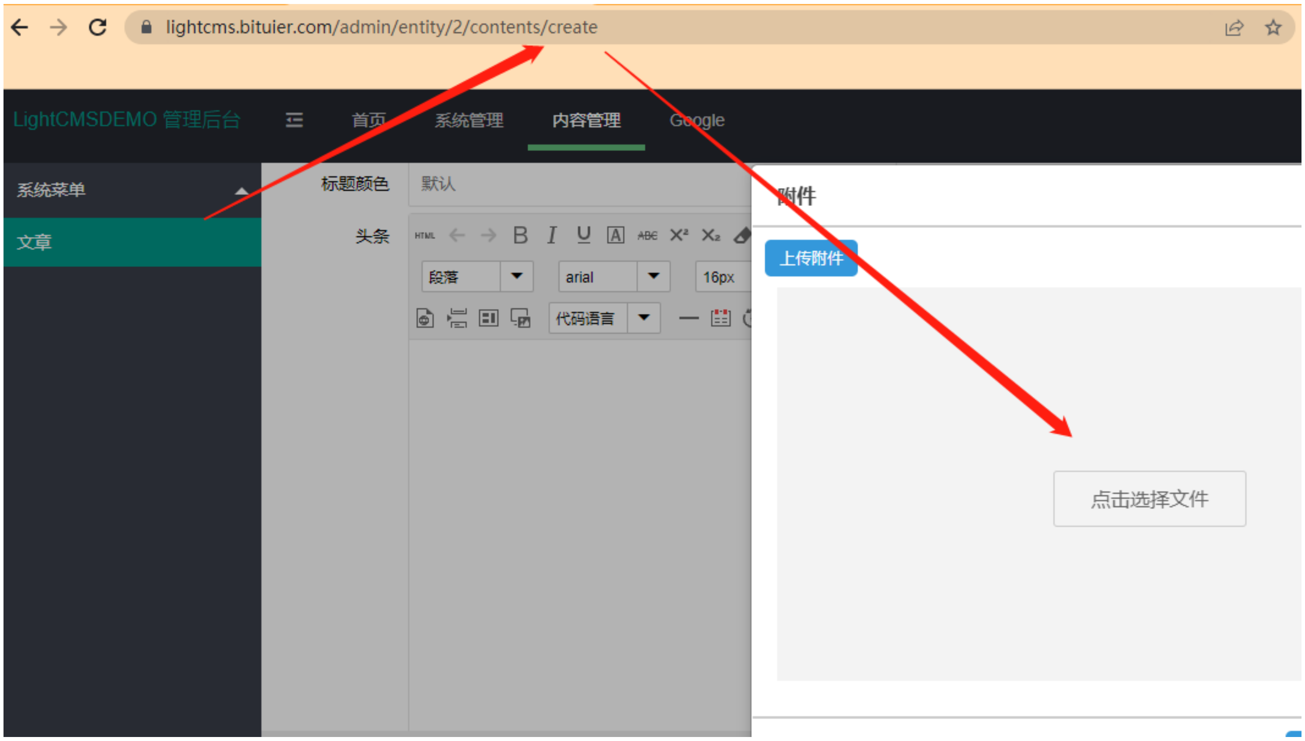
SKdft commented on Jun 6

A stored cross-site scripting (XSS) vulnerability exists in LightCMS that allows an user authorized to upload a malicious .pdf file which acts as a stored XSS payload. If this stored XSS payload is triggered by an administrator it will trigger a XSS attack.

1. login as admin in the article page



2. create a new article

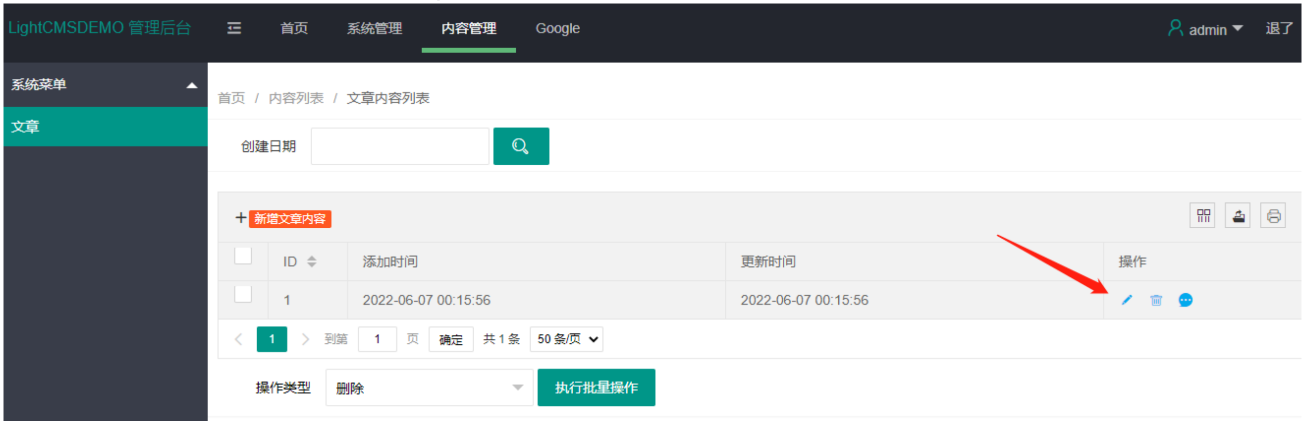


3. upload the malicious pdf. the content of xss.pdf :

```
%PDF-1.4
%1111
1 0 obj
<<
/CreationDate (D:20210619104632+08'00')
/Creator (xss)
/Producer (PDF-XChange Core API SDK \(7.0.324.2\))
>>
endobj
2 0 obj
<<
/Metadata 3 0 R
/Pages 4 0 R
/Type /Catalog
>>
endobj
3 0 obj
<<
/Length 2983
/Subtype /XML
/Type /Metadata
>>
stream
<?xpacket begin="" id="W5M0MpCehiHzreSzNTczkc9d"?>
<x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="XMP Core 5.5.0">
        <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#">
                <rdf:Description rdf:about=""
                                xmlns:dc="http://purl.org/dc/elements/1.1/"
                                xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/"
                                xmlns:xmp="http://ns.adobe.com/xap/1.0/"
```

```
                        xmlns:pdf="http://ns.adobe.com/pdf/1.3/">
                <dc:format>application/pdf</dc:format>
                <xmpMM:DocumentID>uuid:9c93bc08-8e4e-46cb-b28f-
824c693821a4</xmpMM:DocumentID>
                <xmpMM:InstanceID>uuid:2cd63bea-24ca-4ef8-a12c-
015da3b28c96</xmpMM:InstanceID>
                <xmp:CreateDate>2021-06-19T10:46:32+08:00</xmp:CreateDate>
                <xmp:CreatorTool>迅捷PDF编辑器 7.0.324.2</xmp:CreatorTool>
                <xmp:ModifyDate>2021-06-19T10:52:02+08:00</xmp:ModifyDate>
                <pdf:Producer>PDF-XChange Core API SDK (7.0.324.2)</pdf:Producer>
            </rdf:Description>
        </rdf:RDF>
</x:xmpmeta>
```

4. back to content then wo edit this upload:



首页 / 内容列表 / 文章内容列表

创建日期

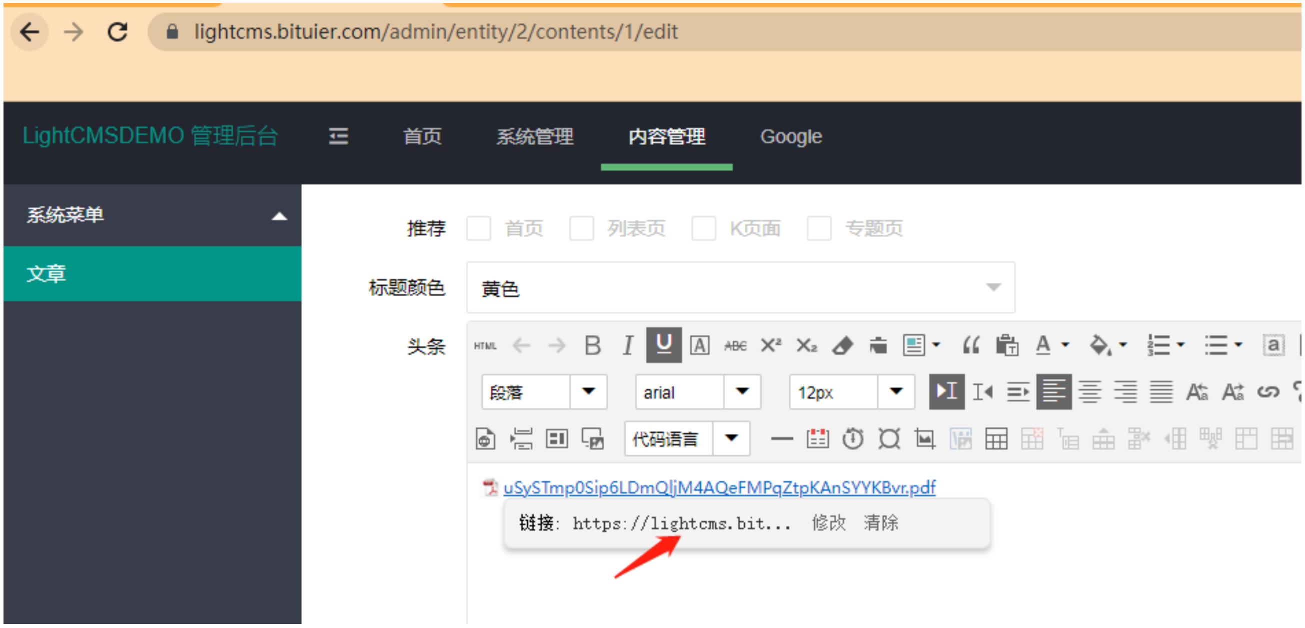
+ 新增文章内容

□	ID	添加时间	更新时间	操作
□	1	2022-06-07 00:15:56	2022-06-07 00:15:56	

1 到第 1 页 确定 共 1 条 50 条/页

操作类型 删除 执行批量操作

5. when user click the link it will trigger a XSS attack



lightcms.bituier.com/admin/entity/2/contents/1/edit

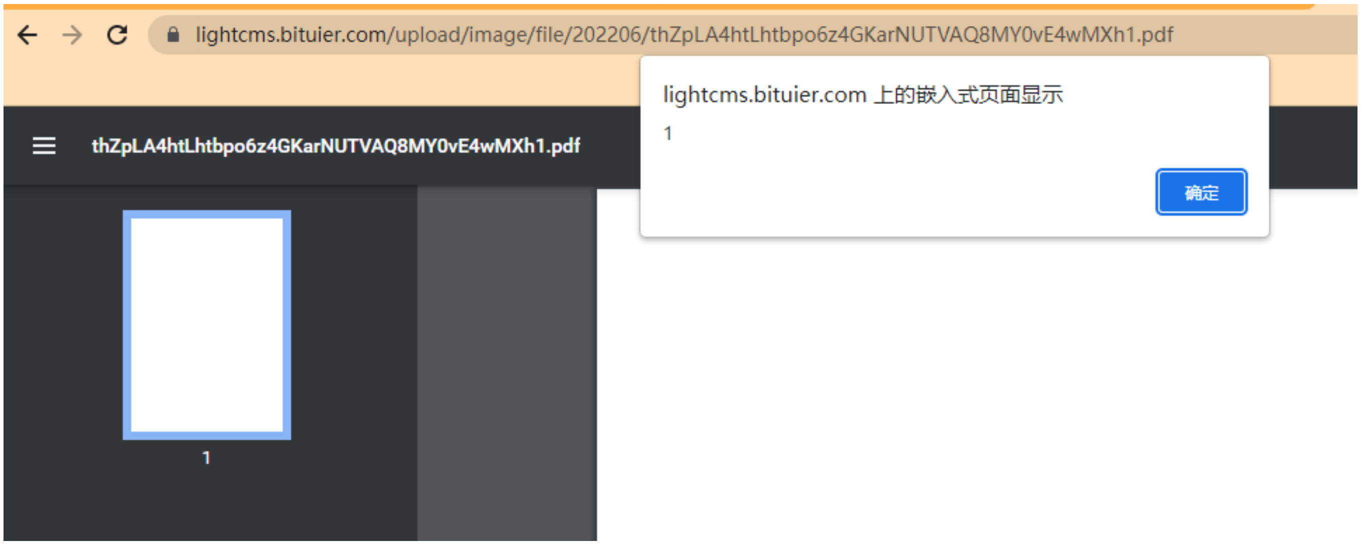
推荐 □ 首页 □ 列表页 □ K页面 □ 专题页

标题颜色 黄色

头条

uSySTmp0Sip6LDmQljM4AQeFMPqZtpKAnSYYKBvr.pdf

链接: https://lightcms.bit... 修改 清除



lightcms.bituier.com/upload/image/file/202206/thZpLA4htLhtbpo6z4GKarNUTVAQ8MY0vE4wMXh1.pdf

thZpLA4htLhtbpo6z4GKarNUTVAQ8MY0vE4wMXh1.pdf

lightcms.bituier.com 上的嵌入式页面显示

1

eddy8 commented on Jun 8 Owner

No better solution have been found except to prohibit users from uploading PDF files, can you give some help to me, thanks.

> Adding the “Content-Disposition: Attachment” and “X-Content-Type-Options: nosniff” headers to the response of static files
> https://owasp.org/www-community/vulnerabilities/Unrestricted_File_Upload

SKdft commented on Jun 8 Author

reference，we recommend the following：

1. nginx configure the reverse proxy which can add a header to the specified url.

```
location /{
    if ($request_filename ~* ^.*?.(txt|doc|pdf|rar|gz|zip|docx|exe|xlsx|ppt|pptx)$){
                    add_header Content-Disposition attachment;
             }
    }
```

2. if it is possible，refer to `https://owasp.org/www-community/vulnerabilities/Unrestricted_File_Upload` --- It is recommended that this practice be performed for all of the files that users need to download in all the modules that deal with a file download.currently we do this.

3.nginx detects the uploaded pdf and find the xss features such as 'app.alert(....)'.

Hope can help you！

👍 1

eddy8 added a commit that referenced this issue on Jun 8

`fix: xss vulnerability #30` ✓ ca904a6

eddy8 closed this as completed on Jun 8

eddy8 added a commit that referenced this issue on Jul 7

`fix: xss vulnerability #30` b316a46

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants