**山东省教育行业网络安全通报**

山东省教育厅

2020年12月23日

# 一. 事件概况

**测试机构：** 淄博师范高等专科学校

**测试范围：** wlkc.zbnc.edu.cn

经过测试，该机构网站系统包含如下风险：

|  |  |  |
| --- | --- | --- |
| No. | 漏洞名称 | 漏洞危害 |
| 1 | 弱口令+存储xss | 低危 |

# 二. 漏洞详情

**1.弱口令漏洞**

201305030117 密码是学号  
201305030120,201305030231,201305030240,201305030320等账户都在下面连接，账户泄露在这：<http://pes.zbnc.edu.cn/content.jsp?urltype=news.NewsContentUrl&wbtreeid=1071&wbnewsid=2327>

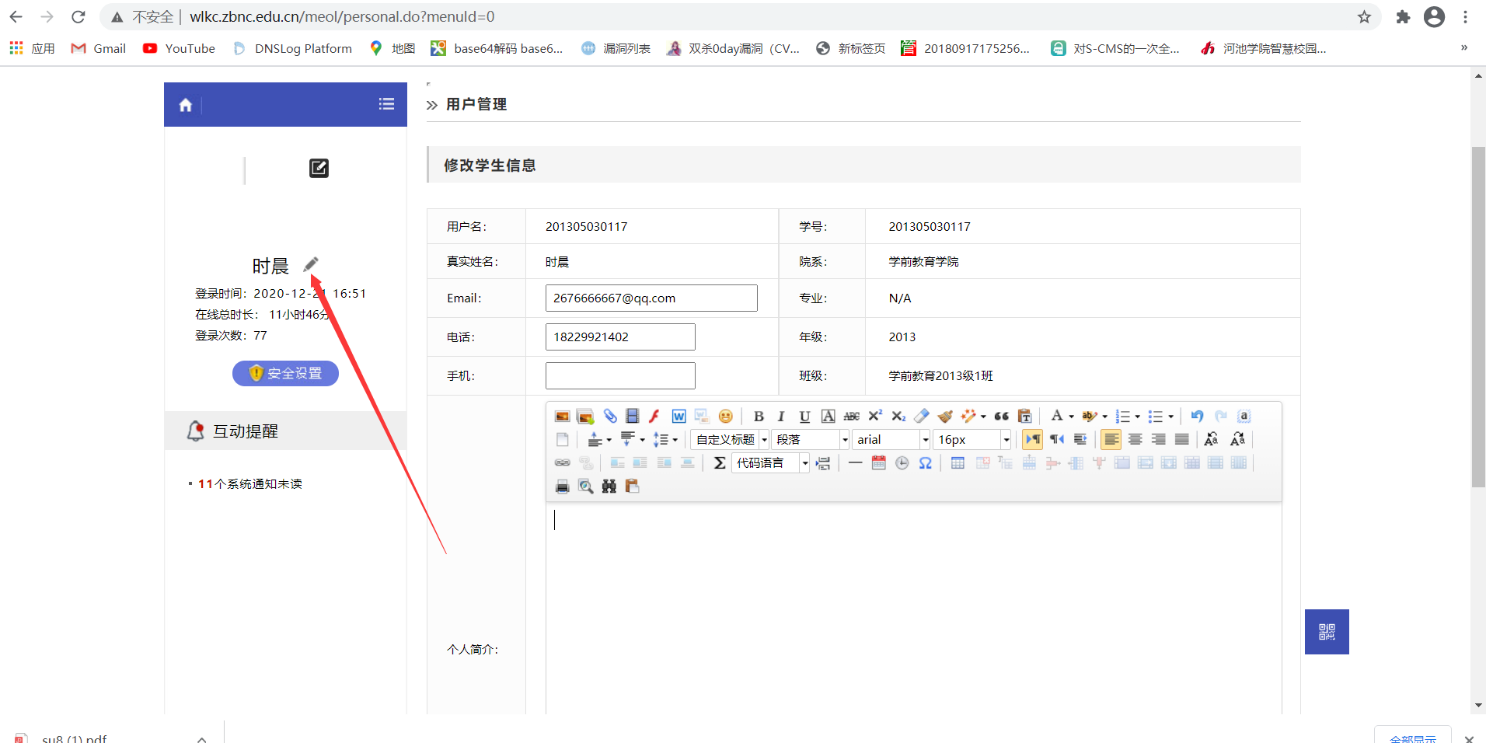
学号就是密码

**2.XSS：**

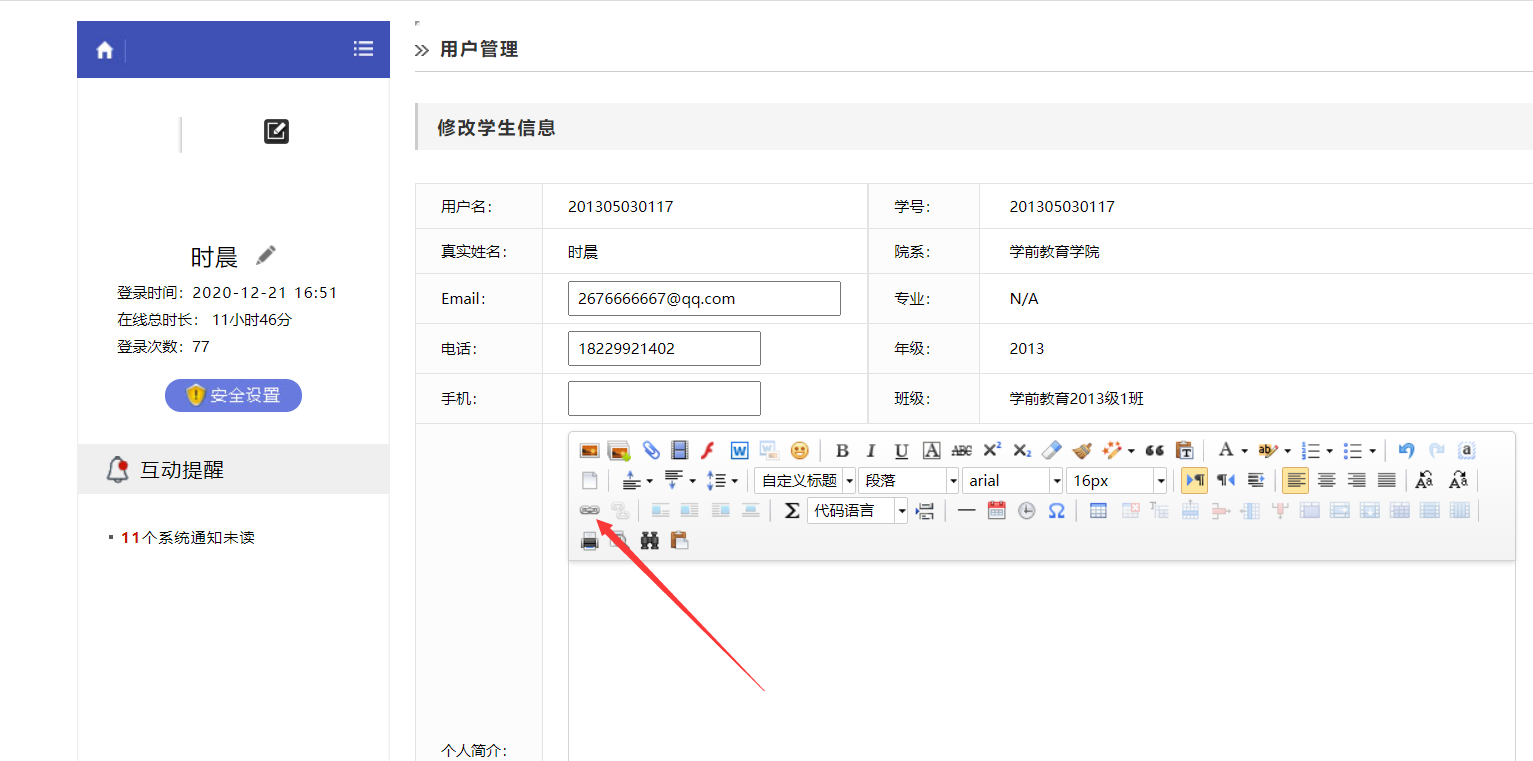
<http://wlkc.zbnc.edu.cn/>

先用这个账户201305030117登录进去

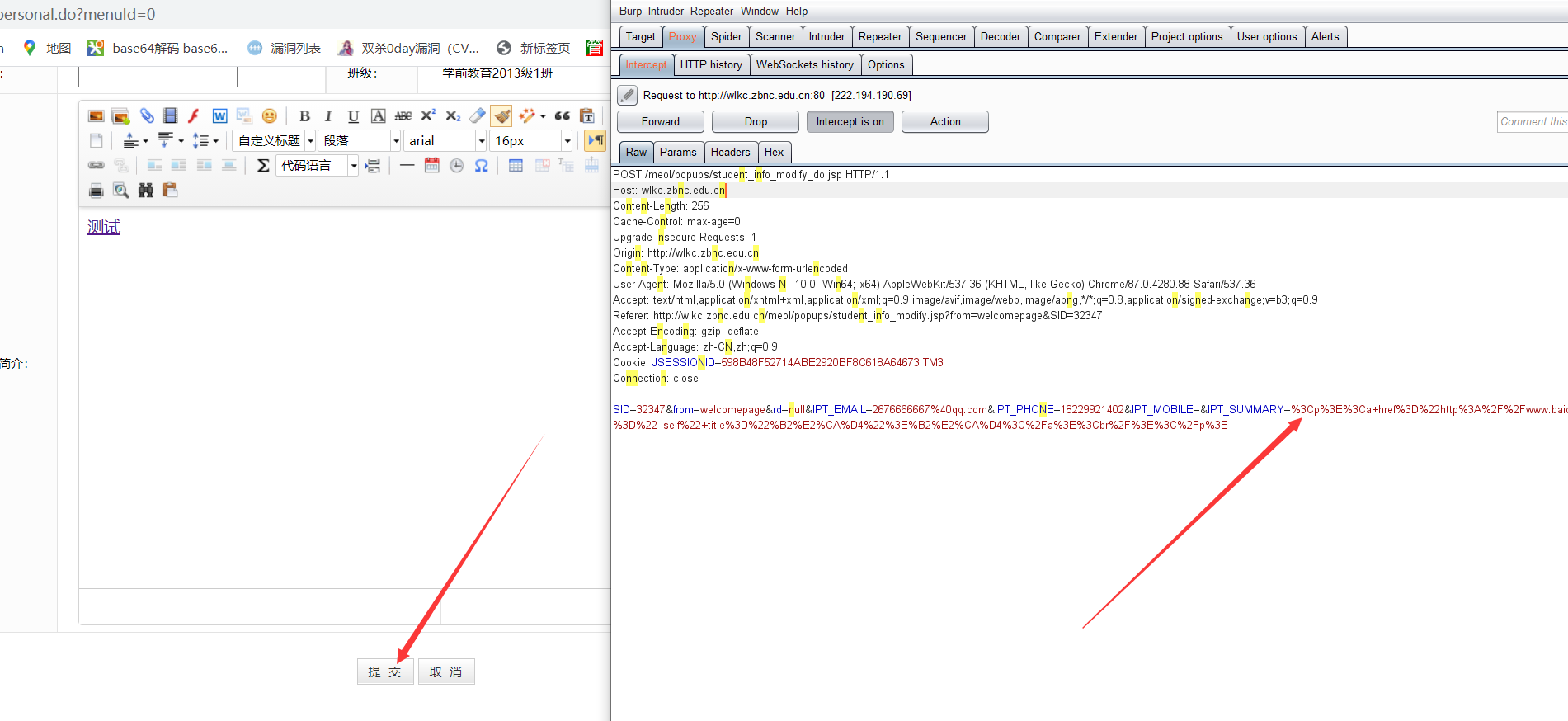
先点击修改



然后超链接，超链接里面内容随便写

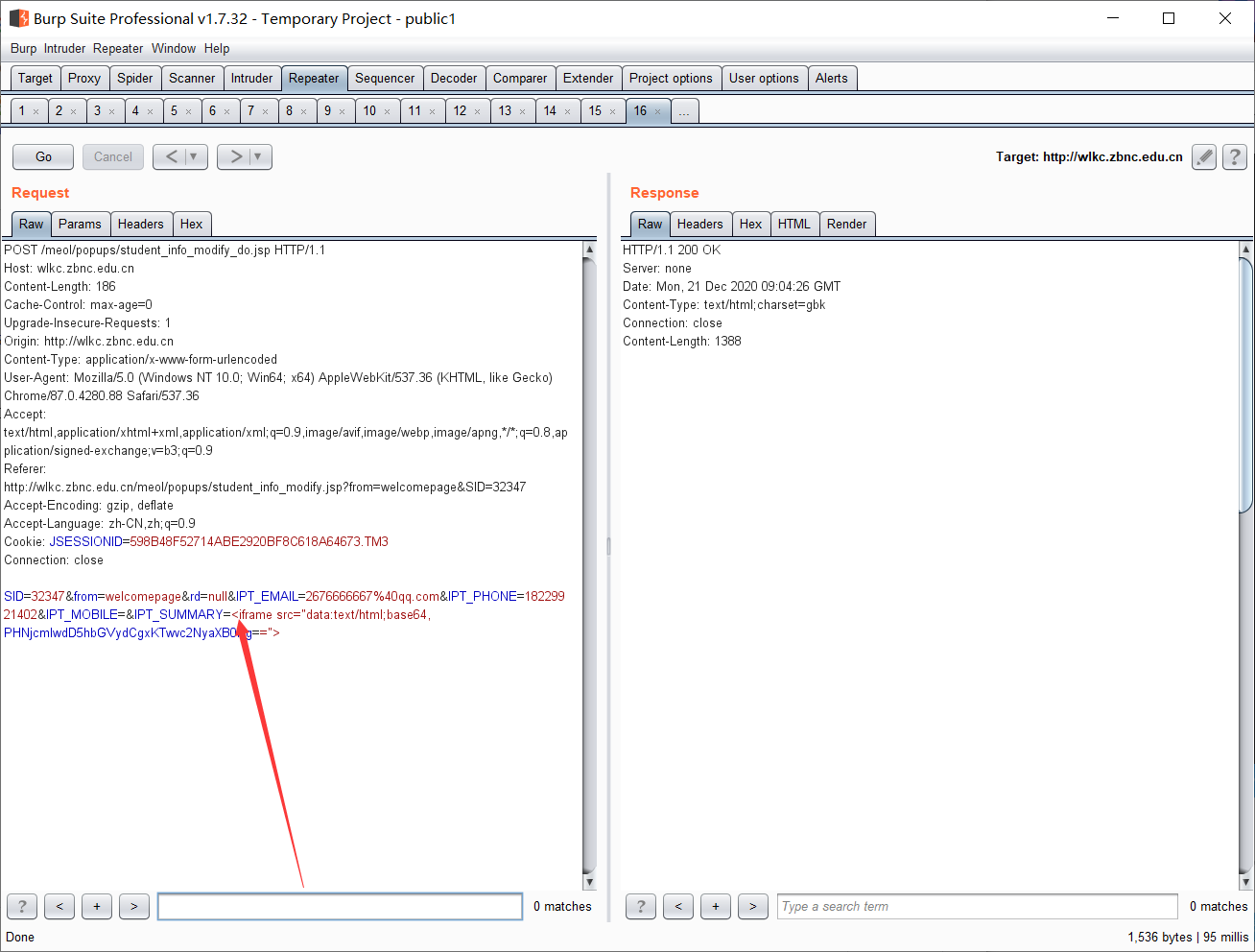


然后保存抓包



改成<iframe src="data:text/html;base64,PHNjcmlwdD5hbGVydCh4c3MpPC9zY3JpcHQ+">

加密的明文是<script>alert(1)</script>



网页被挂非法弹窗：

