上海商学院

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

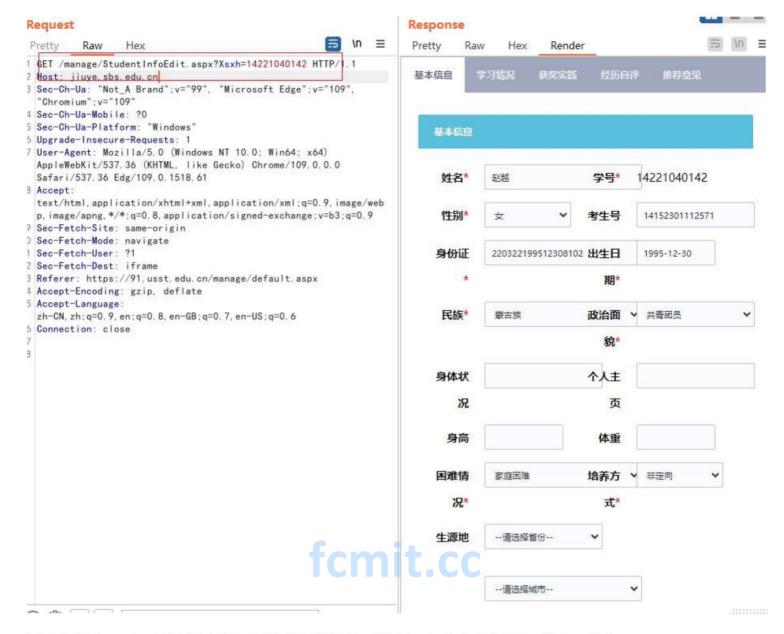
3.资产确认:



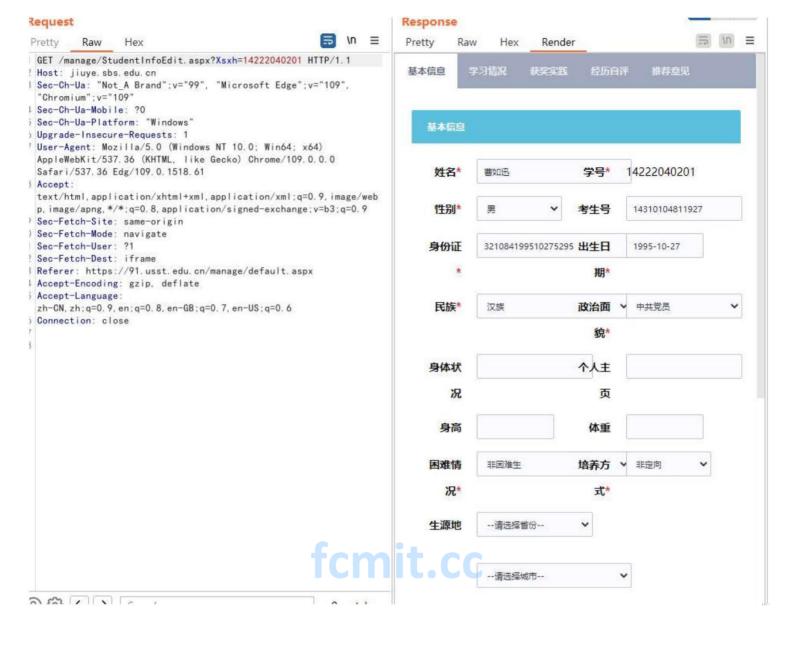
4.漏洞详情:

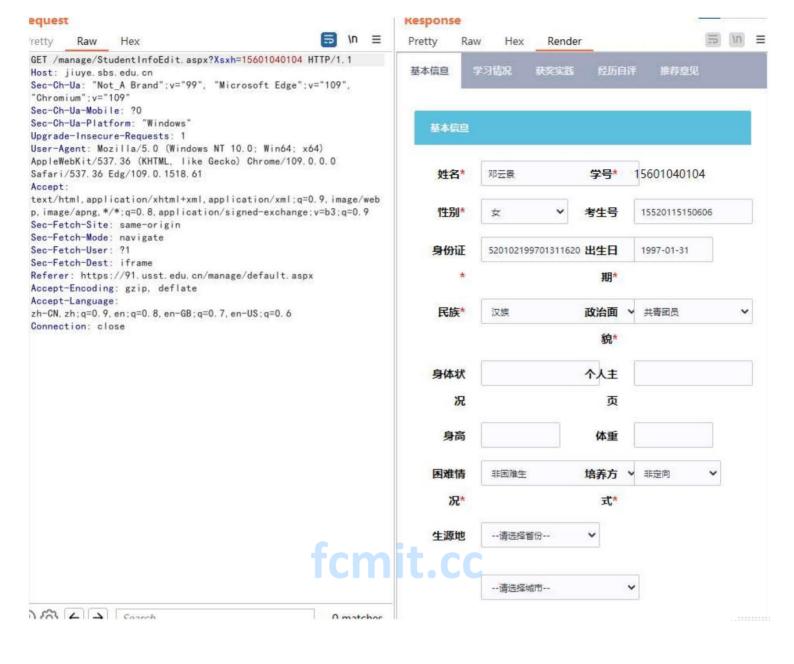
(1) 第一处接口未授权:

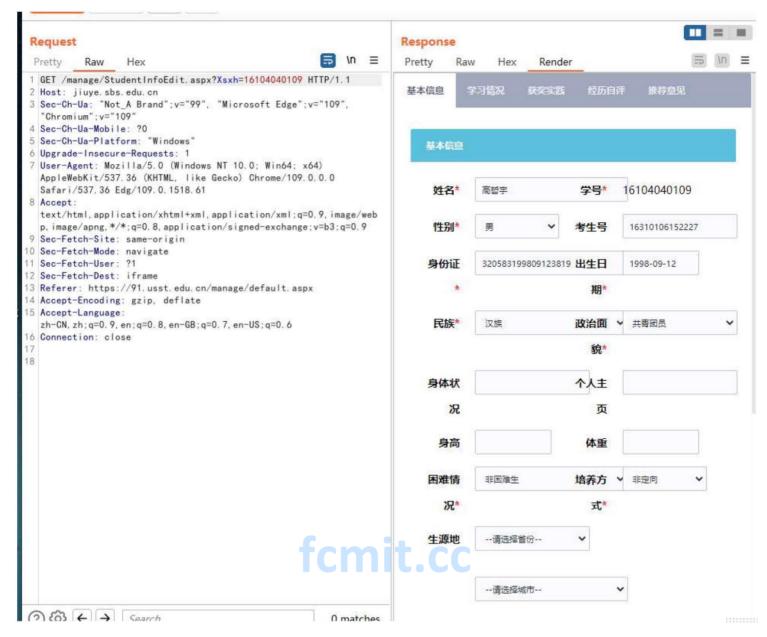
/manage/StudentInfoEdit.aspx?Xsxh=14221040142



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:



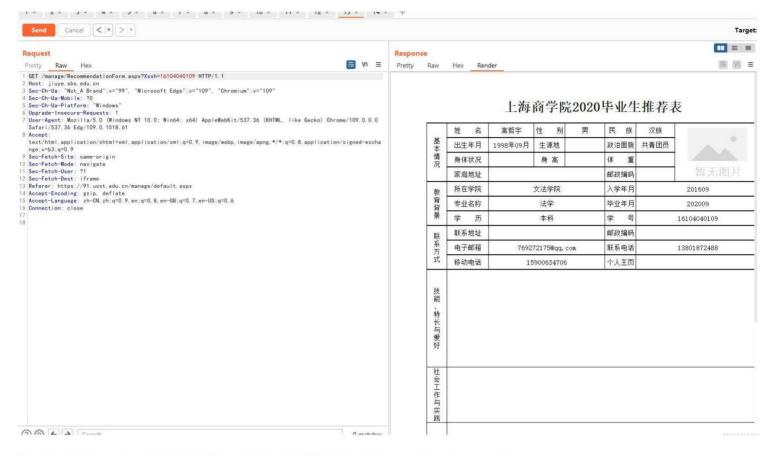




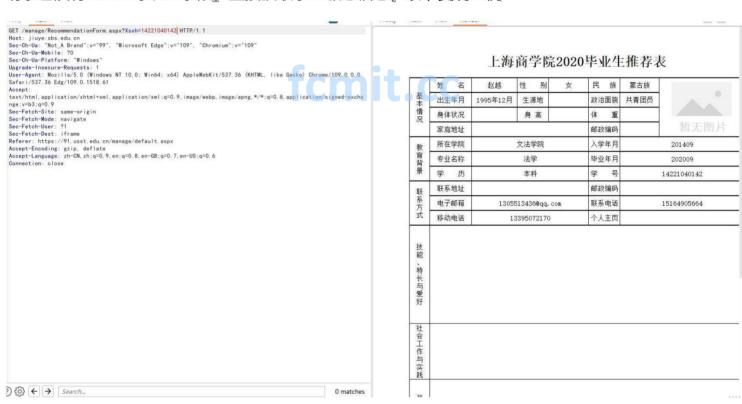
学号来自谷歌信息收集。理论上可以通过做学号字典可以遍历全校学生个人信息

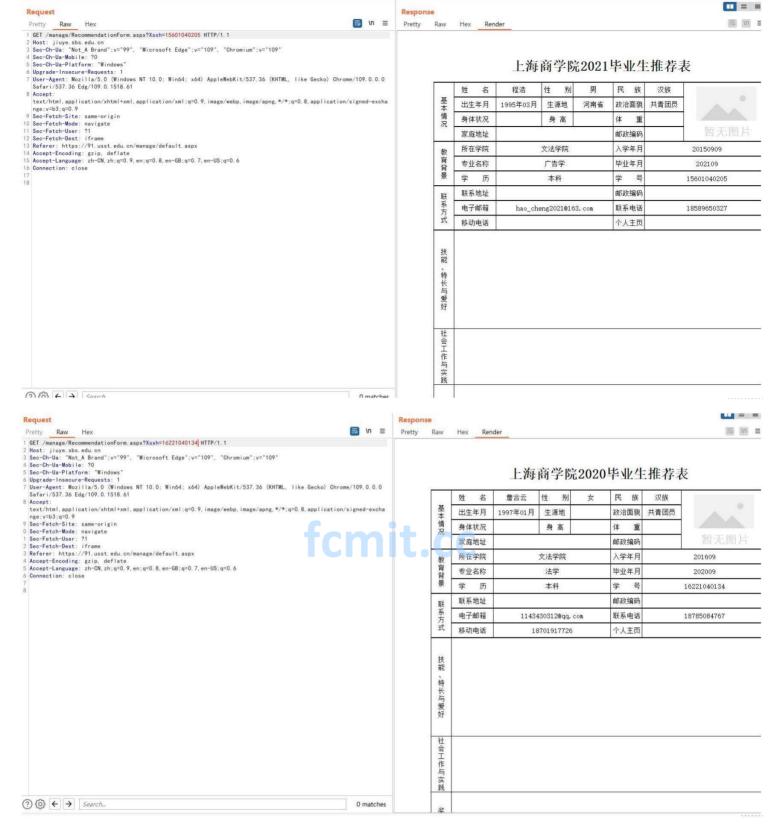
(2) 第二处接口未授权:

/manage/RecommendationForm.aspx?Xsxh=16104040109



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:





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

2023 © 联系邮箱: contact@src.sjtu.edu.cn (mailto:contact@src.sjtu.edu.cn)

fcmit.cc