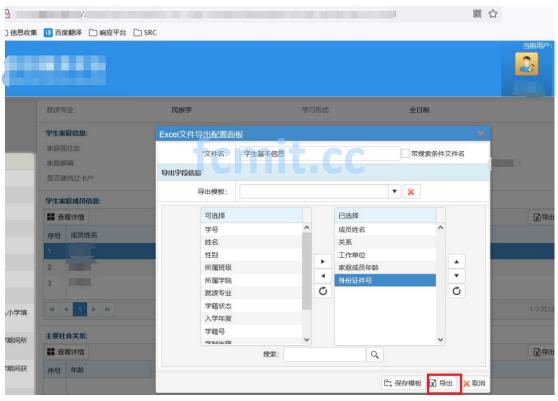
2.点击个人信息 -> 学生基本信息 -> 找到家庭成员信息, 导出 excel



3.点击导出 excel, 把身份证号加入导出行列, 点击导出抓包。数据包里面出现身份证号和学号对应, 学号





4.因为系统不允许重复放包,重复放包会显示500错误。所以每次导出就要重新点击导出。 我们再次执行上述操作。抓包 我们把参数 student_uuid 后面的值改为: STUDENT-20190516-117293010121,放包



改为: STUDENT-20190516-117293010120



5.成功造成水平越权,通过漏洞可以遍历全校学生身份证号,造成大量身份证泄露