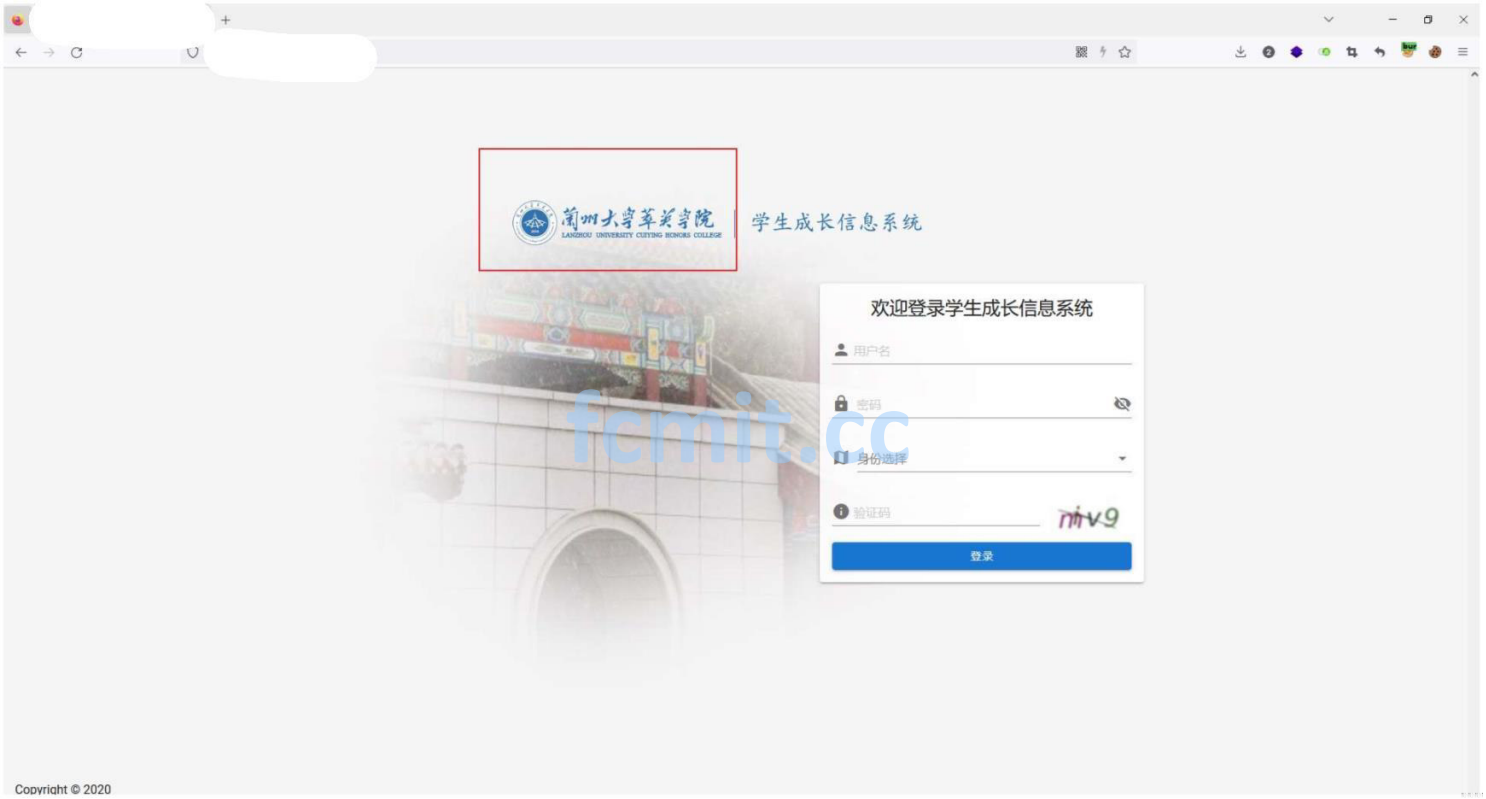
兰州大学

存在漏洞

漏洞地址：

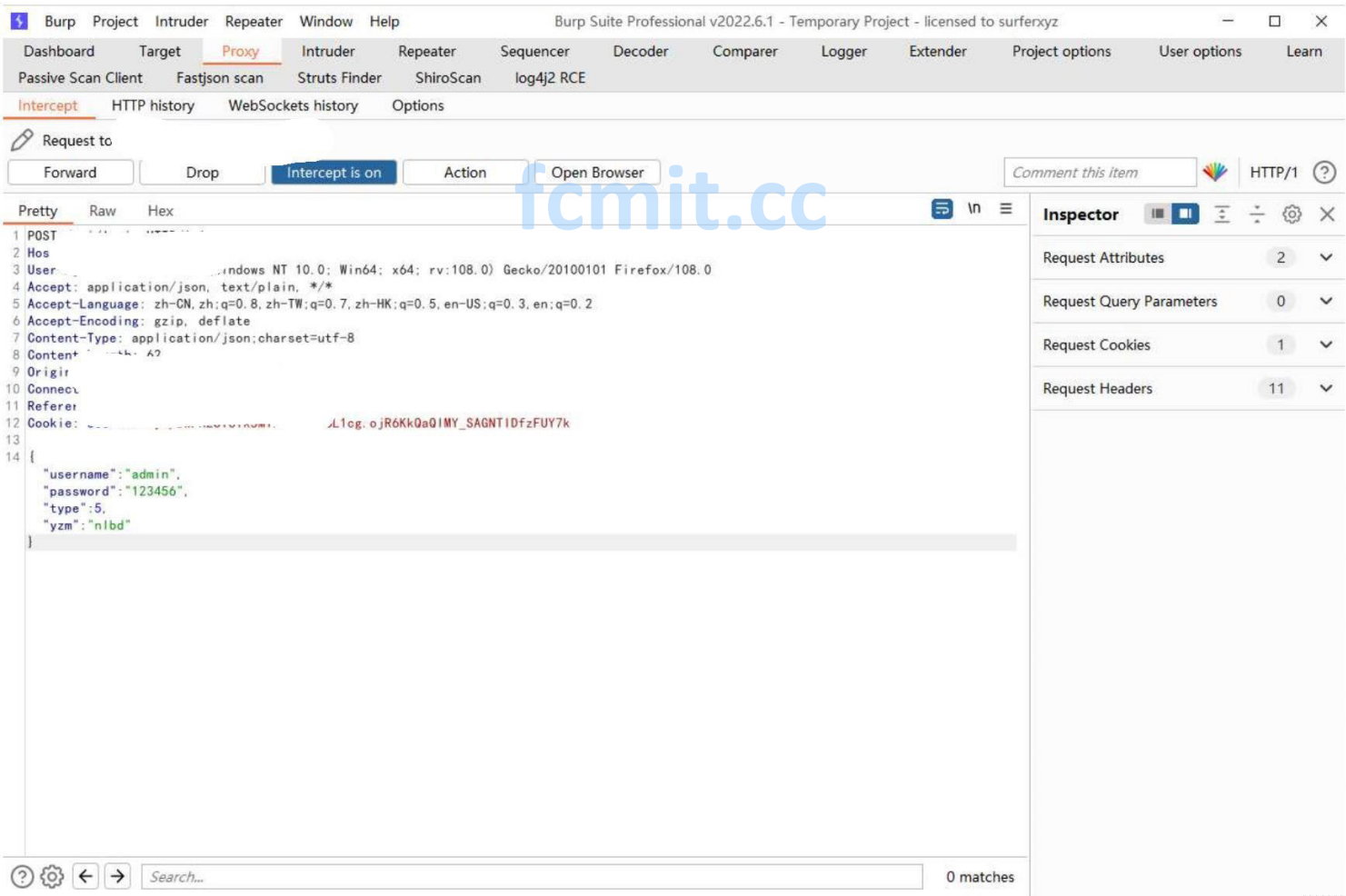
漏洞名称：兰州大学萃英学院学生成长信息系统存在逻辑漏洞进入管理系统批量添加管理用户

资产确认：

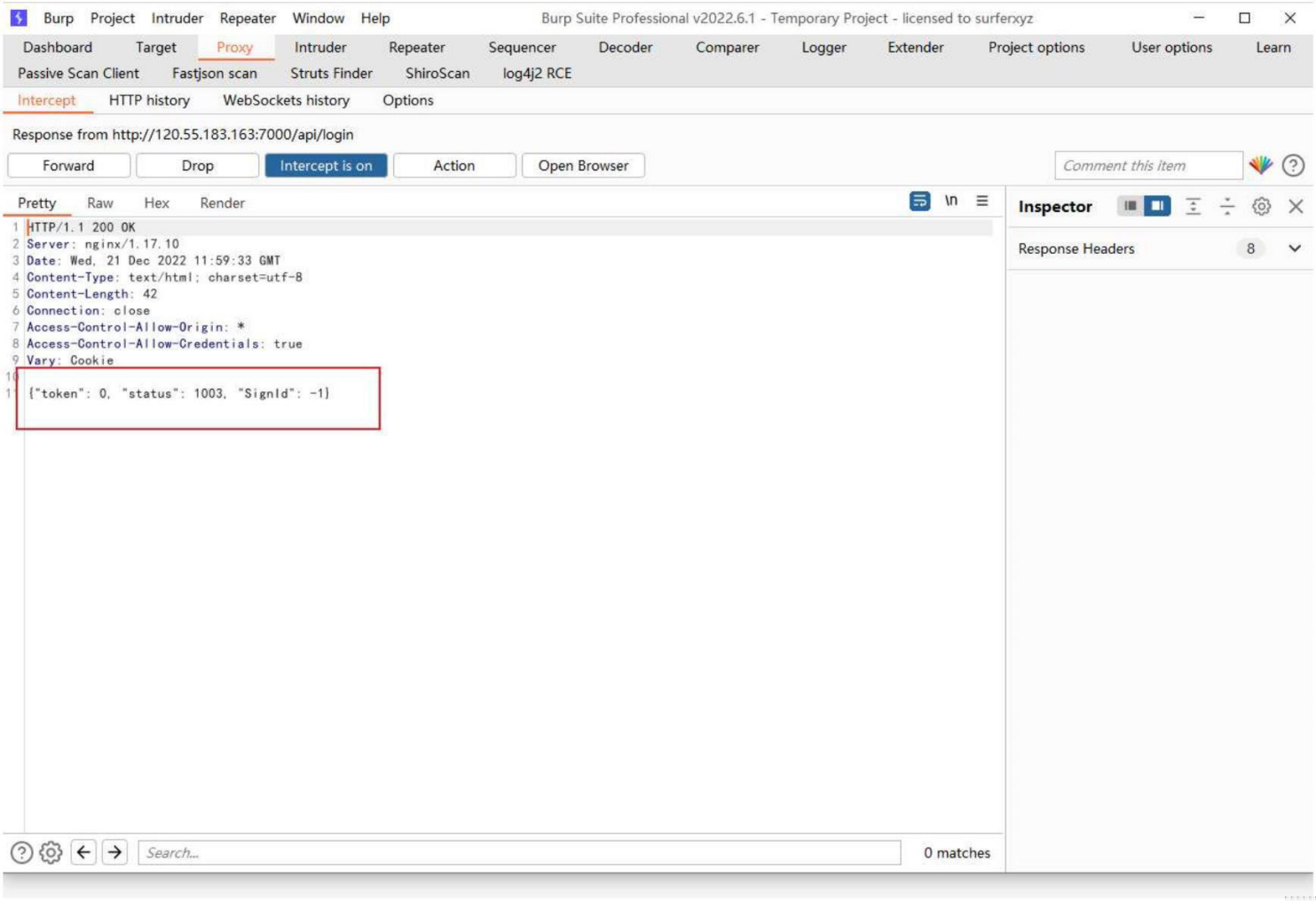


漏洞详情：

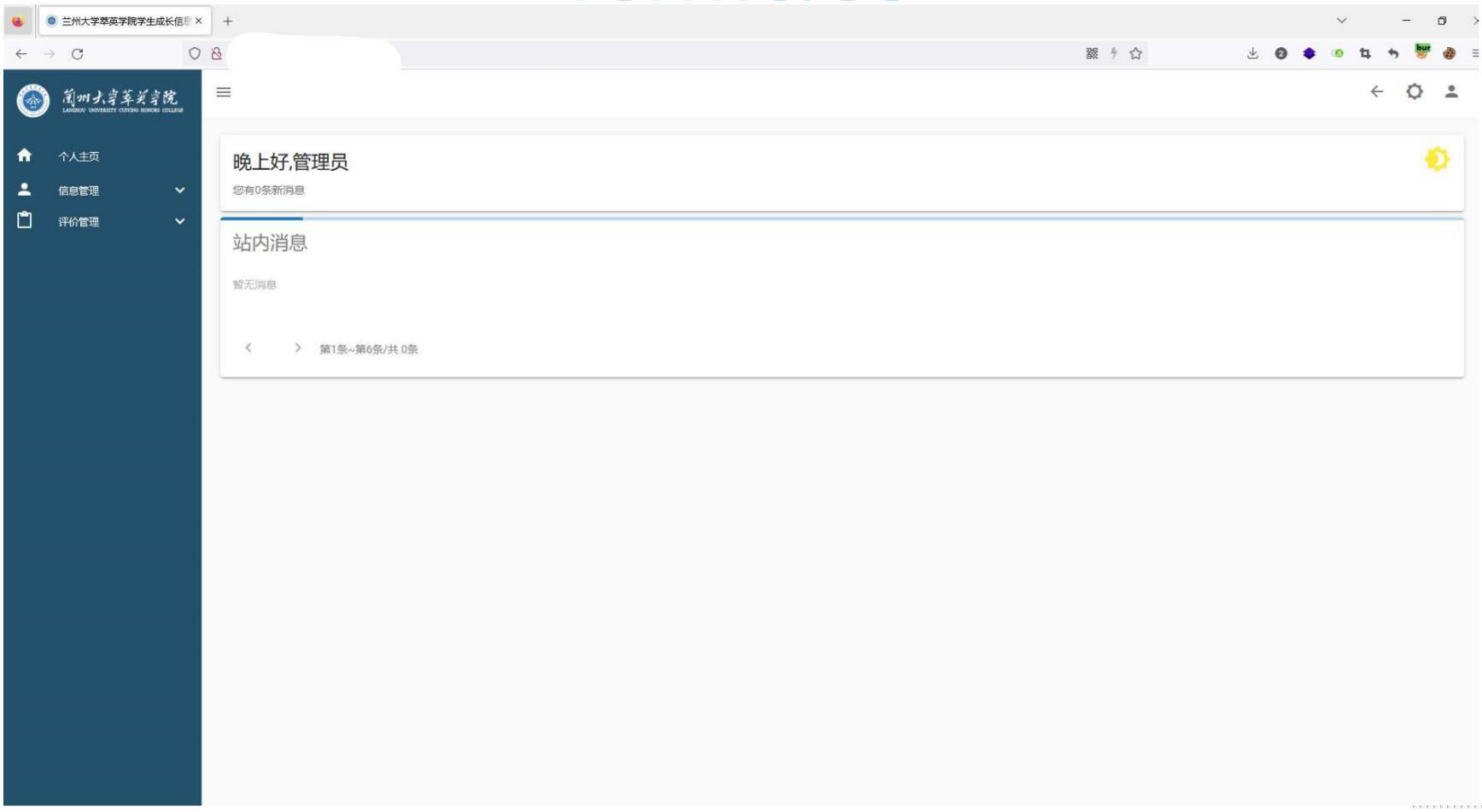
（1）在登陆处输入账号密码admin/123456,选择管理员，写验证码，抓登陆包如下所示：



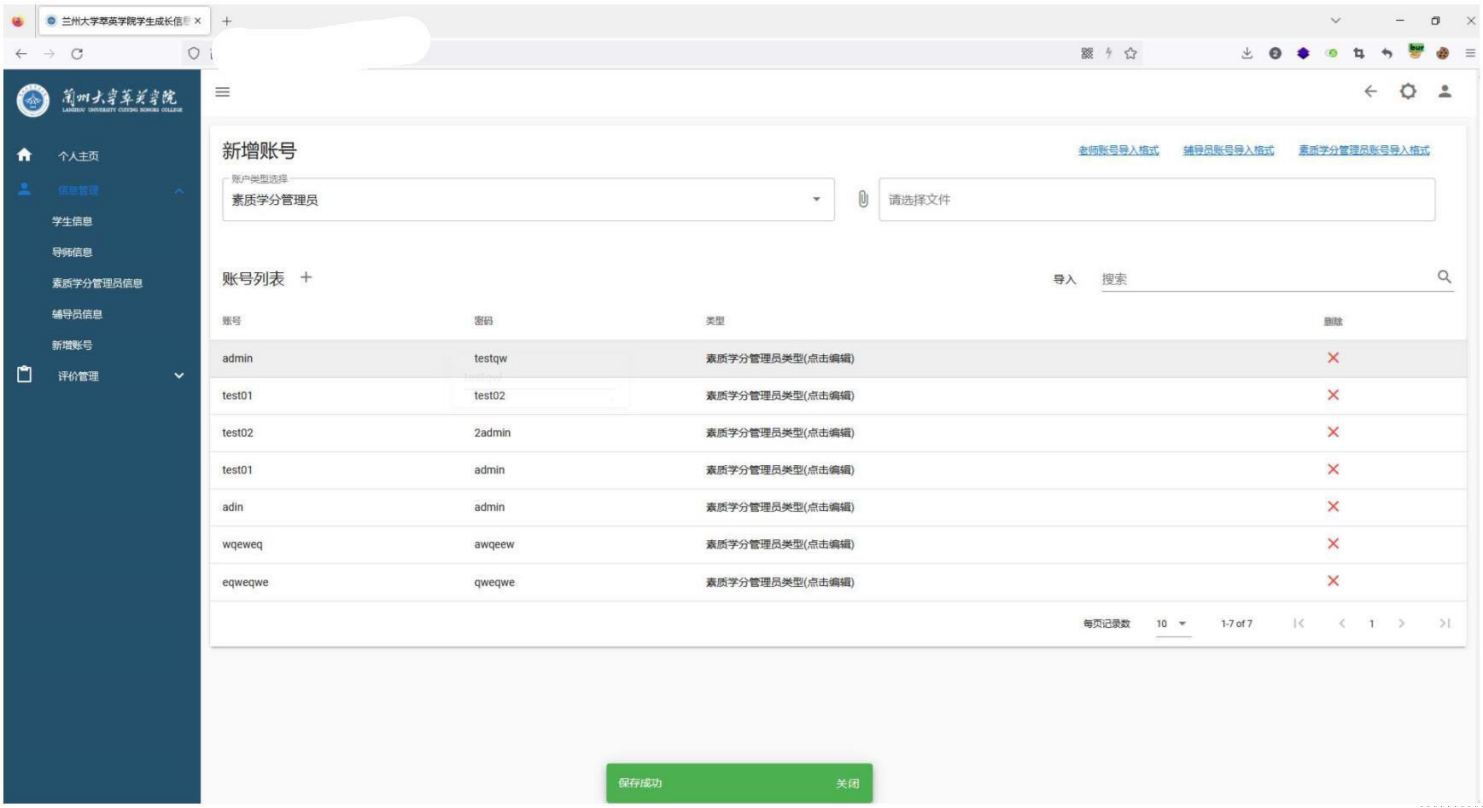
然后拦截响应报文，把status改成1000，SignId改成1然后放包



随后直接进入管理后台，身份为管理员



点击信息管理->新增账号，随便测试了几个，素质学分管理员，辅导员，教师均可添加账号密码



已添加的账号已经已经自行删除，恢复原样，未对其他模块内容进行删除，添加，修改的操作

修复建议：建议对登陆数据包进行严格校验，未授权用户添加相关302跳转，对登陆逻辑进行修改，以防攻击者登入管理后台进行恶意利用。