tomcat远程代码执行漏洞（cve-2017-12615）

一 介绍

当 Tomcat 运行在 Windows 主机上，且启用了 HTTP PUT 请求方法（例如，将readonly 初始化参数由默认值设置为 false），攻击者将有可能可通过精心构造的攻击请求向服务器上传包含任意代码的 JSP 文件。之后，JSP 文件中的代码将能被服务器执行。

二 影响版本

Apache Tomcat 7.0.0 - 7.0.79

三 分析

tomcat配置文件中的readonly设置为false时，攻击者可以通过put请求创建恶意jsp文件，但是tomcat处理http请求用到的servlet为DefalutServlet和JspServlet，前者是处理静态资源（html,image）,后者是处理动态资源（jsp，jspx），同时处理put请求的是DefalutServlet，因此直接上传jsp恶意文件是不会成功的，所以还需要结合文件名解析漏洞来触发该漏洞。

四 复现场景

攻击机：kali 192.168.23.18

靶机：win10 192.168.22.253

五 复现

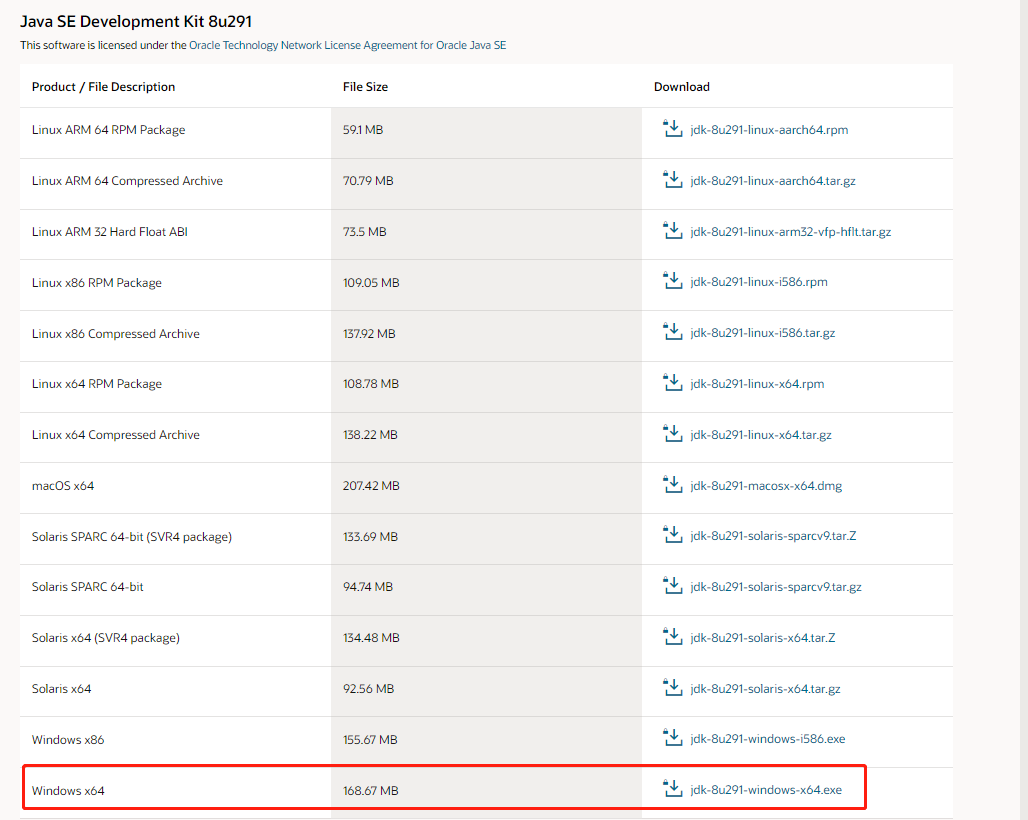
1 环境搭建

tomcat 7.0.75

jdk1.8

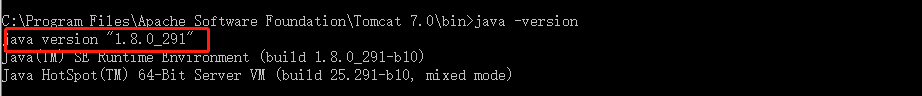
a 安装jdk

https://www.oracle.com/cn/java/technologies/javase/javase-jdk8-downloads.html



需要注册oracle账号才能够下载

下载完成之后直接安装下一步直至安装完成，注意需要记住安装的路径，tomcat安装是需要用到。



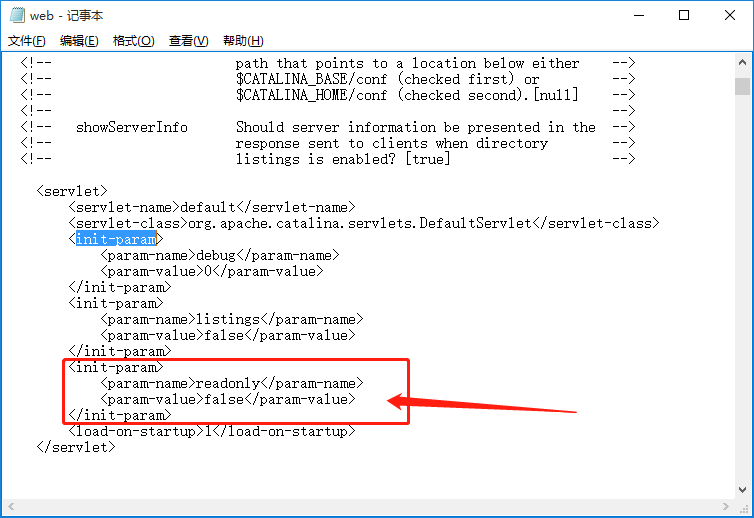
b tomcat安装

<http://www>.ouyaoxiazai.com/soft/stgj/133/45254.html

下载完也是直接下一步直至完成，中间的jdk安装路径需要填对。

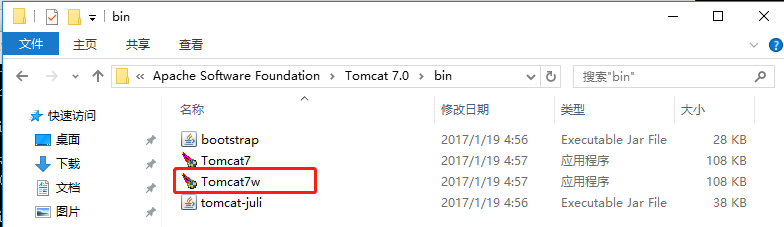
c 修改tomcat配置文件

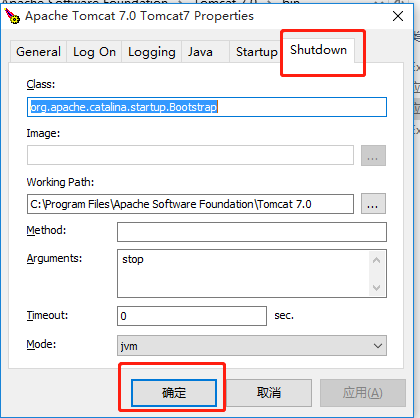
进入tomcat安装路径，进入conf文件夹，打开web.xml配置文件，搜索‘init-param’,添加字段readonly，值为false。

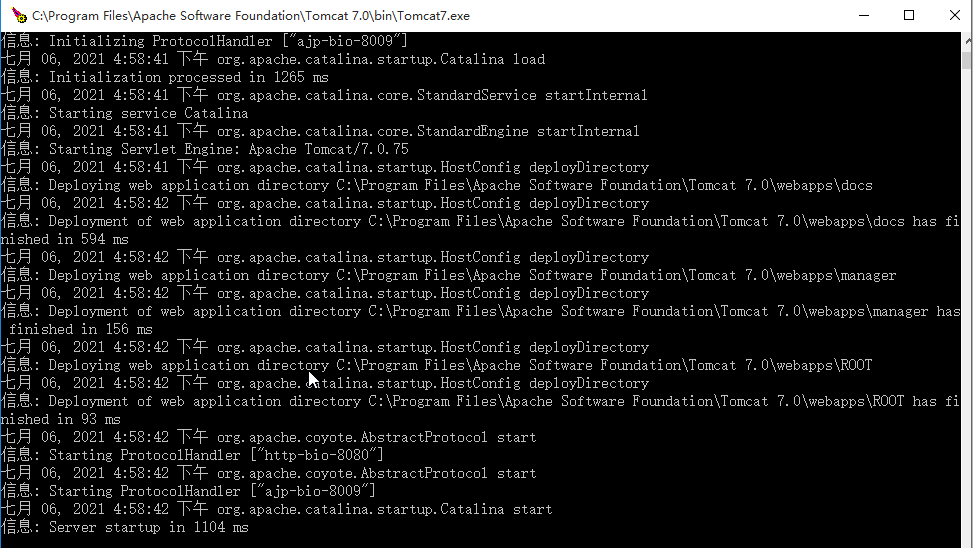


d 重启tomcat

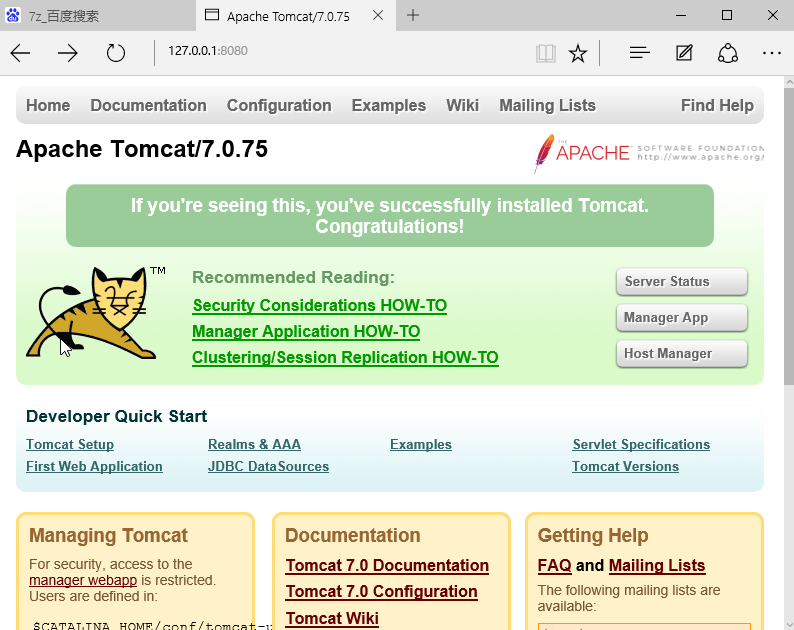
进入bin文件夹，双击Tomcat7w文件，进入如下菜单选择确定，然后再点击Tomcat7，即重新启动tomcat服务。





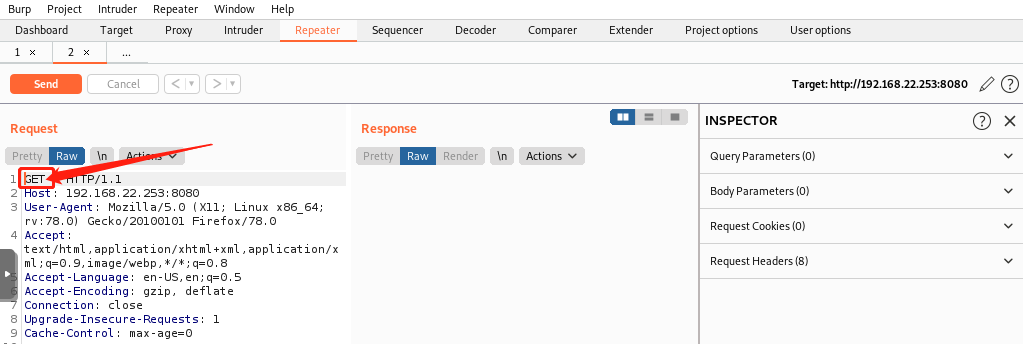


访问loaclhost:8080即可

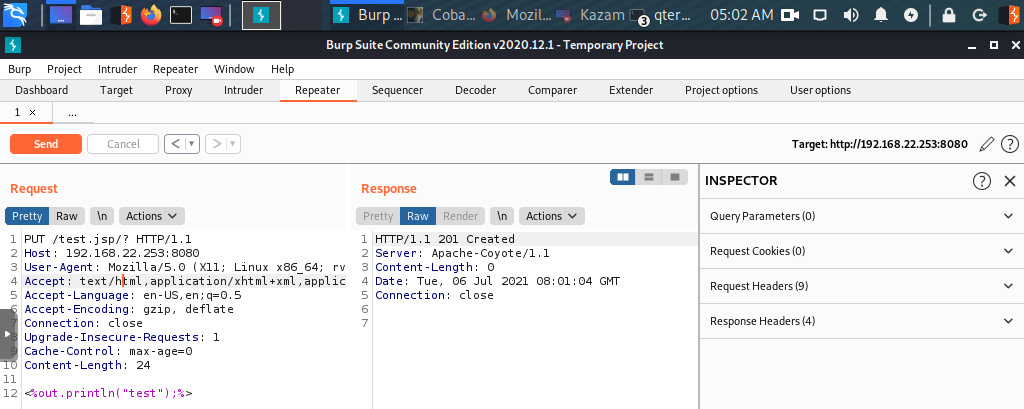


2 攻击流程

a 在kali机中设置代理，启动burpsuite，刷新tomcat页面，拦截http get请求，重放。

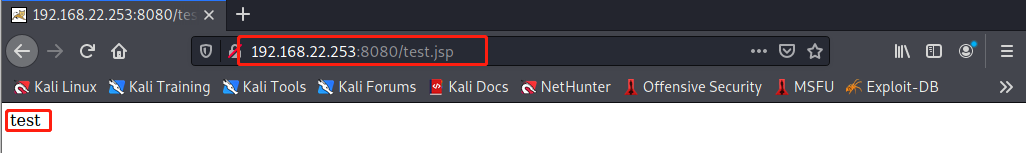


b 如下图修改get请求为put请求，put后面接jsp脚本文件名，记得加‘/’（文件名解析漏洞绕过利用），接着在请求最后输入脚本的内容（shell），send即可，返回200或者201为成功，返回404或者405等其他响应码为失败。



c 如果创建成功，则可以在浏览器中访问该文件

如果脚本的内容为shell的话，访问之后就可以上线。



可以在此处看到我创建的test.jsp文件。

