Tomcat7+ 弱口令 && 后台getshell漏洞

环境说明

Tomcat7+权限分为:

- manager (后台管理)
 - o manager-gui 拥有html页面权限
 - o manager-status 拥有查看status的权限
 - o manager-script 拥有text接口的权限,和status权限
 - o manager-jmx 拥有jmx权限,和status权限
- host-manager (虚拟主机管理)
 - o admin-gui 拥有html页面权限
 - o admin-script 拥有text接口权限

这些权限的作用可以查看: http://tomcat.apache.org/tomcat-8.5-doc/manager-howto.html。

在 conf/tomcat-users.xml 文件中配置用户的权限:

可见,用户tomcat拥有上述所有权限,密码是 tomcat 。

正常安装的情况下,tomcat8中默认没有任何用户,且manager页面只允许本地IP访问。只有管理员手工修改了这些属性的情况下,才可以进行攻击。

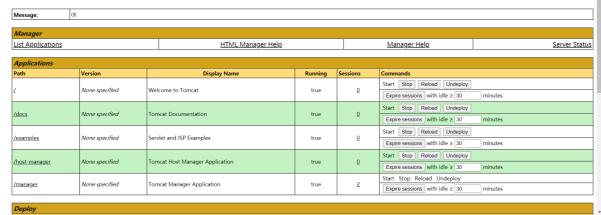
漏洞测试

打开tomcat管理页面 http://your-ip:8080/manager/html ,输入弱密码 tomcat:tomcat ,即可访问后台:

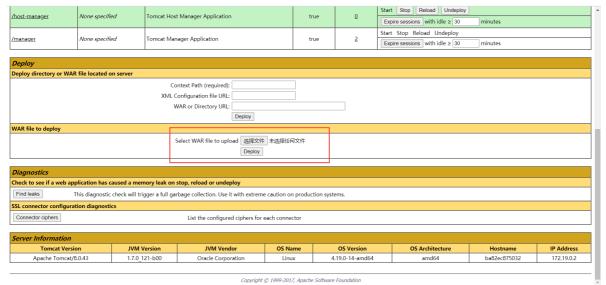




Tomcat Web Application Manager



下面有一个文件上传:



coppigit (2000 confide t

上传一个 .war 包即可Getshell。