Tomcat7_weakpasswd 弱口令 漏洞复现

原创

ADummy_ 于 2021-02-04 12:27:27 发布 284 收藏

分类专栏： vulhub_Writeup 文章标签： 网络安全 渗透测试 安全漏洞

本文链接：https://blog.csdn.net/weixin_43416469/article/details/113636325

Tomcat 7 +弱口令

by ADummy

0x00利用路线

tomcat弱口令登录后台—>后台具有上传文件的功能—>上传木马—>getshell

0x01漏洞介绍

Apache+Tomcat是很常用的网站解决方案，Apache用于提供web服务，而Tomcat是Apache服务器的扩展，用于运行jsp页面和servlet。Tomcat有一个后台管理界面，使用具有权限的用户登录后台，可上传war包(webshell)部署到web目录下。getshell

0x02前置知识

1.什么是war包？

war包是用来进行Web开发时一个网站项目下的所有代码,包括前台HTML/CSS/JS代码,以及后台JavaWeb的代码。 当开发人员开发完毕时,就会将源码打包给测试人员测试,测试完后若要发布则也会打包成War包进行发布。War包 可以放在Tomcat下的webapps或word目录,当Tomcat服务器启动时，War包即会随之解压源代码来进行自动部署。

2.如何得到弱口令？

1.使用burpsuite爆破

2.使用msf自带模块进行爆破 auxiliary/scanner/http/tomcat_mgr_login

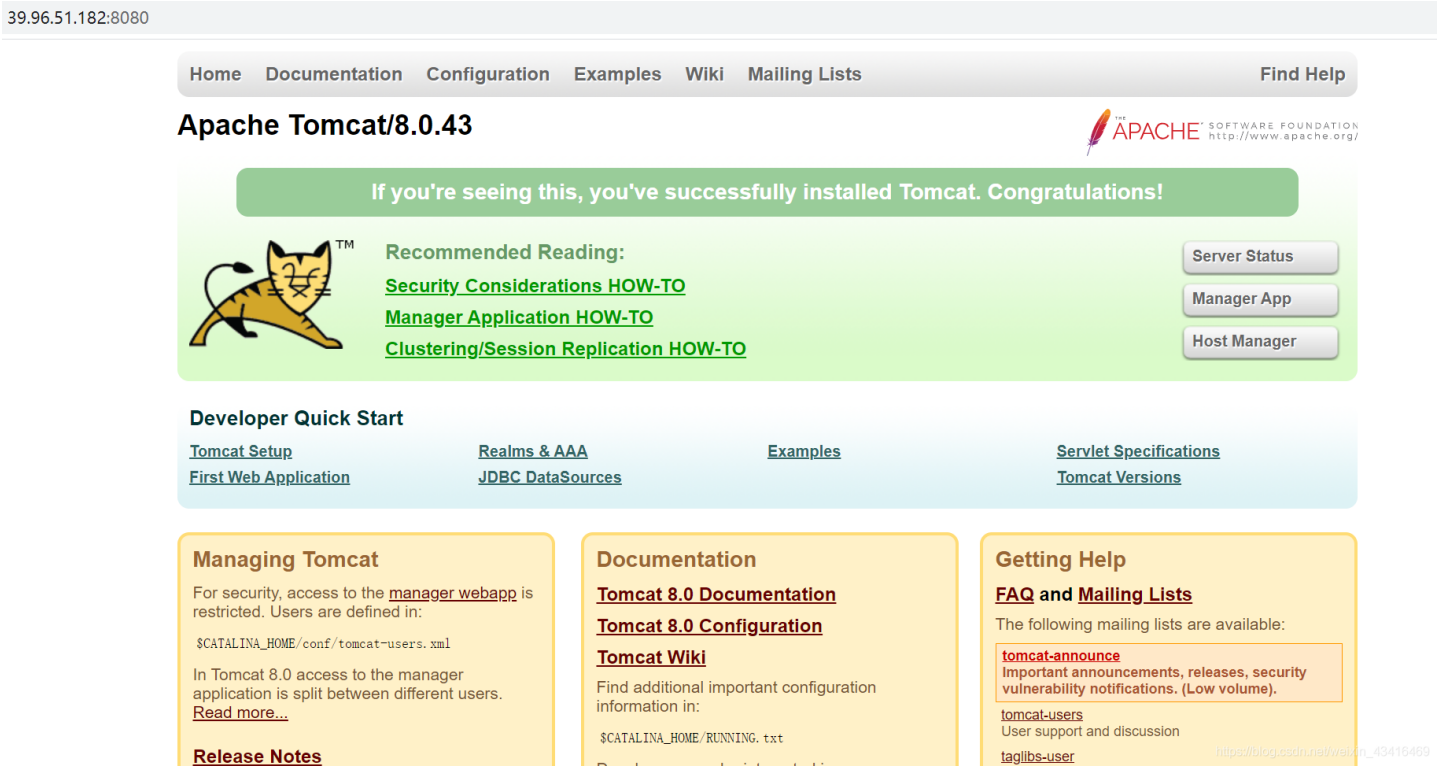
3.tomcat会针对登陆次数过多的用户进行锁定，经过统计分析，当登录错误>5次后，就会锁定用户。如何绕过？ 以上请自行百度

3.不是本地登录可以上传war包吗？

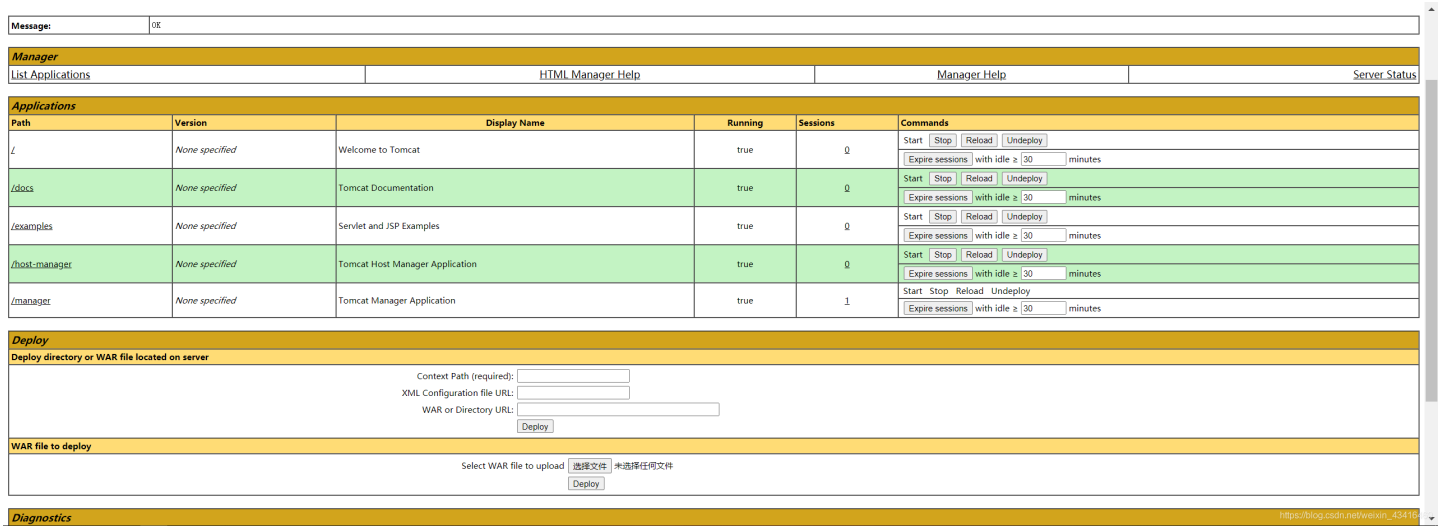
正常安装的情况下，tomcat8中默认没有任何用户，且manager页面只允许本地IP访问。只有管理员手工修改了这些属性的情况下，才可以进行攻击

0x03复现过程

打开tomcat管理页面 `http://your-ip:8080`
点击Manager App 输入弱口令，进入管理界面



将准备好的jsp一句话木马，压缩成zip格式，修改后缀名成为.war文件，上传一句话。



Message: OK

Manager

List Applications | HTML Manager Help | Manager Help | Server Status

Applications

Path	Version	Display Name	Running	Sessions	Commands
/	None specified	Welcome to Tomcat	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/docs	None specified	Tomcat Documentation	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/examples	None specified	Servlet and JSP Examples	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/host-manager	None specified	Tomcat Host Manager Application	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/manager	None specified	Tomcat Manager Application	true	1	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes

Deploy

Deploy directory or WAR file located on server

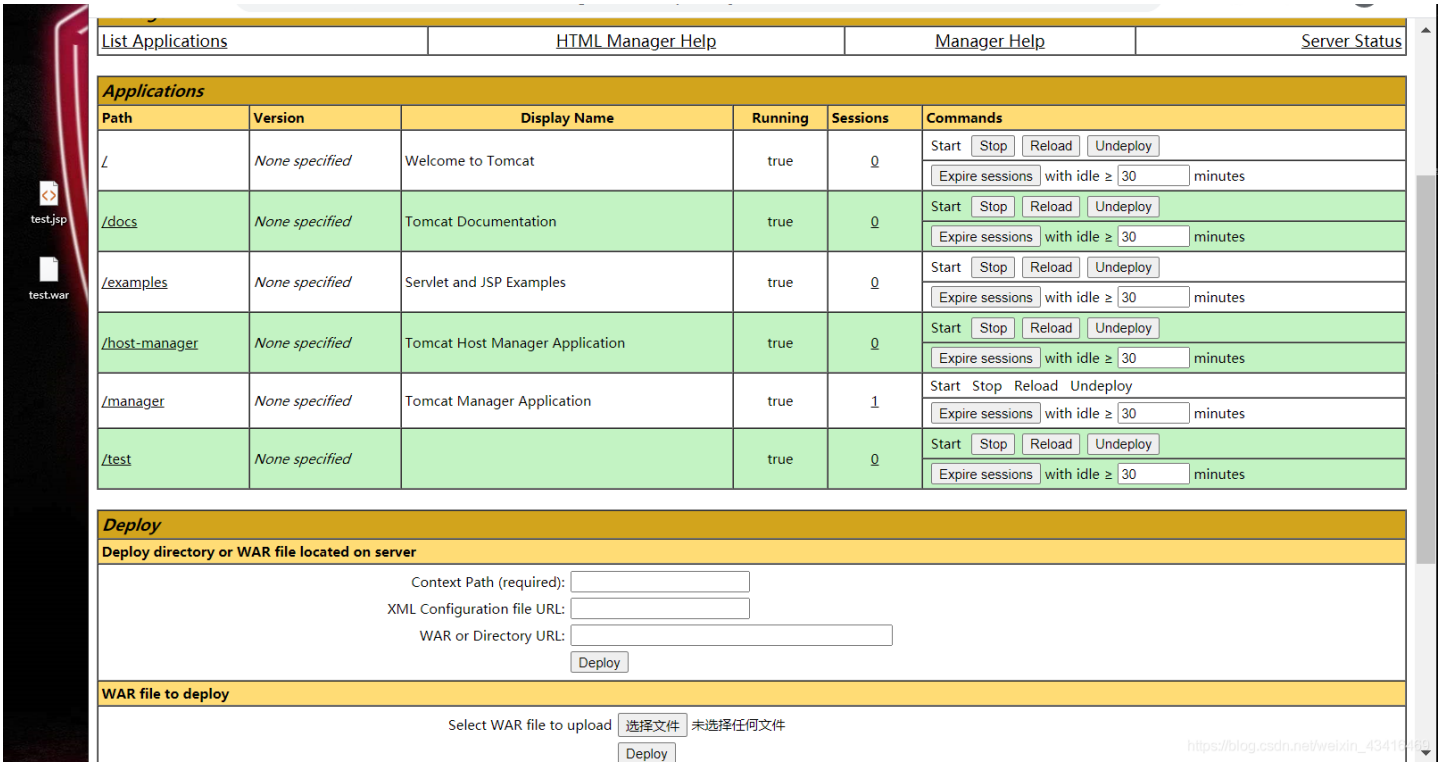
Context Path (required):
XML Configuration file URL:
WAR or Directory URL:
Deploy

WAR file to deploy

Select WAR file to upload 选择文件 未选择任何文件
Deploy

Diagnostics

可以看到，Path 增加了一个/test目录



test.jsp

test.war

List Applications | HTML Manager Help | Manager Help | Server Status

Applications

Path	Version	Display Name	Running	Sessions	Commands
/	None specified	Welcome to Tomcat	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/docs	None specified	Tomcat Documentation	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/examples	None specified	Servlet and JSP Examples	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/host-manager	None specified	Tomcat Host Manager Application	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/manager	None specified	Tomcat Manager Application	true	1	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/test	None specified		true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes

Deploy

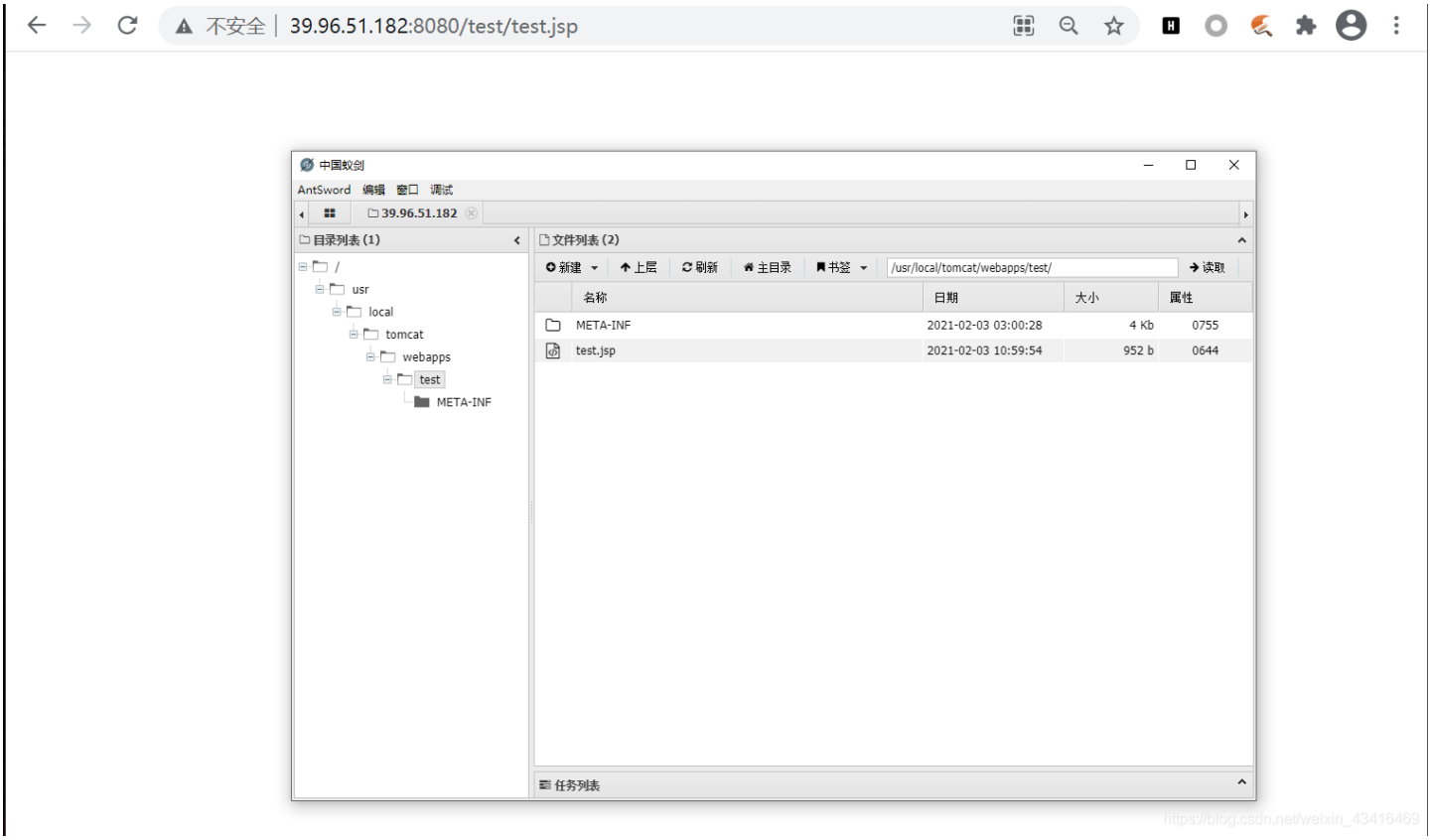
Deploy directory or WAR file located on server

Context Path (required):
XML Configuration file URL:
WAR or Directory URL:
Deploy

WAR file to deploy

Select WAR file to upload 选择文件 未选择任何文件
Deploy

访问/test/test.php,使用蚁剑连接。(笔者找了好多jsp的一句话，有的不可用，找了一个比较好的分享给大家，文章结尾有链接。)



至此 getshell。

0x04总结

这是笔者的第一次文章，耗时一整天左右。对笔者来说意义很大，收获颇多。笔者完全从一个初学者的角度，梳理了复现漏洞的全部流程，并做了一点点拓展。由于笔者水平有限，不能像大佬一样做很多的拓展，但是我觉得，能来打靶场的人初学者居多，拓展更多的是抛砖引玉的作用。本文在创作的时候也参考了各个师傅的文章。衷心感谢。

0x05参考资料

https://www.cnblogs.com/bmjoker/p/9892653.html

https://www.cnblogs.com/qianxinggz/p/13440366.html

jsp：
https://github.com/ADummmy/vulhub_Writeup/tree/main/code/Tomcat7_weakpasswd_jsp.jsp

所有的writeup，方便下载，留存。
https://github.com/ADummmy/vulhub_Writeup