01-开班第一课

目录

**[一、](#_Toc138683320)****[作业内容](#_Toc138683320)** [3](#_Toc138683320)

[1. xxxx 3](#_Toc138683321)

[2. xxxxx 3](#_Toc138683322)

[3. …… 3](#_Toc138683323)

**[二、](#_Toc138683324)****[操作步骤](#_Toc138683324)** [4](#_Toc138683324)

[1. xxxxx 4](#_Toc138683325)

[2. xxxxx 4](#_Toc138683326)

[3. …… 4](#_Toc138683327)

**[三、](#_Toc138683328)****[作业总结](#_Toc138683328)** [5](#_Toc138683328)

[1. xxxxx 5](#_Toc138683329)

[2. xxxxx 5](#_Toc138683330)

[3. …… 5](#_Toc138683331)

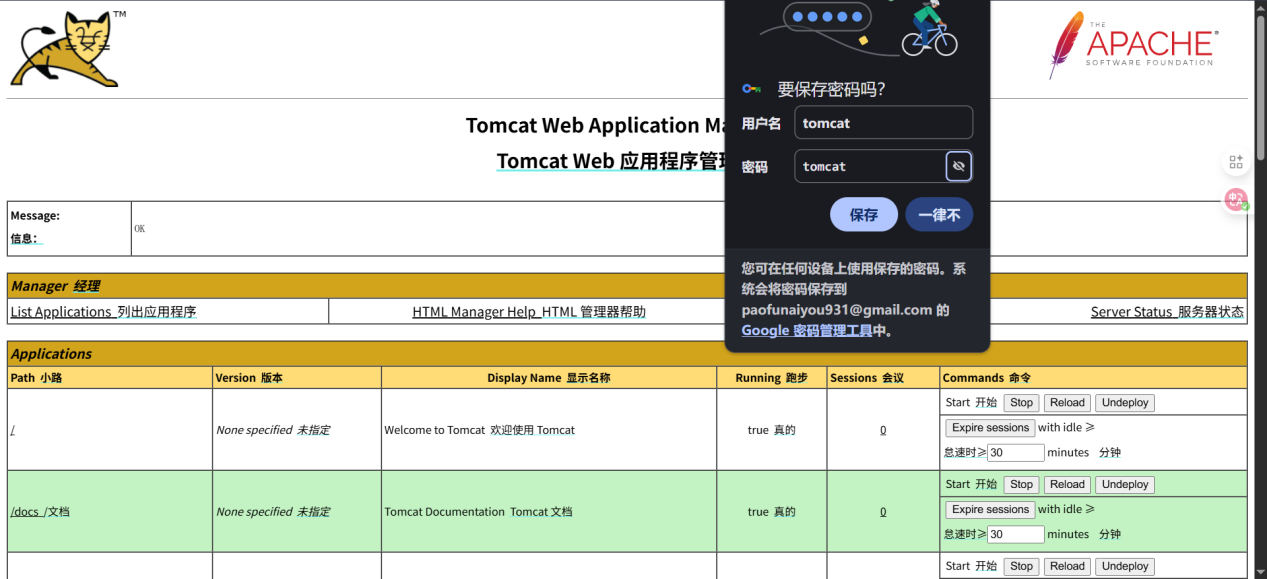
1. **作业内容**

开启实验tomcat8并获取该机器服务器权限

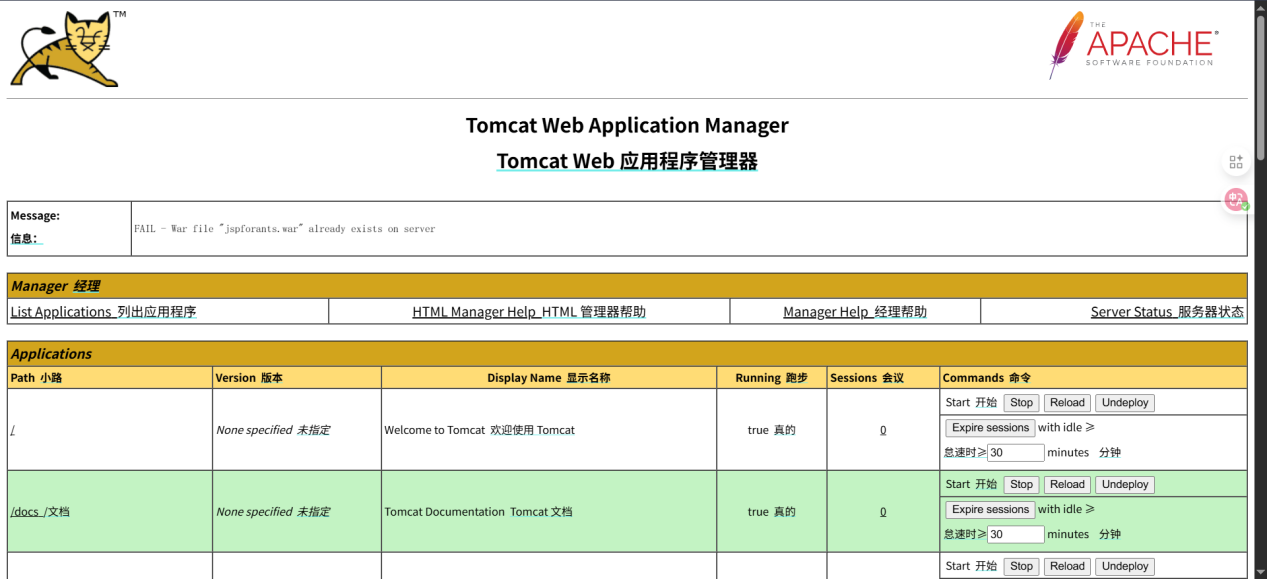
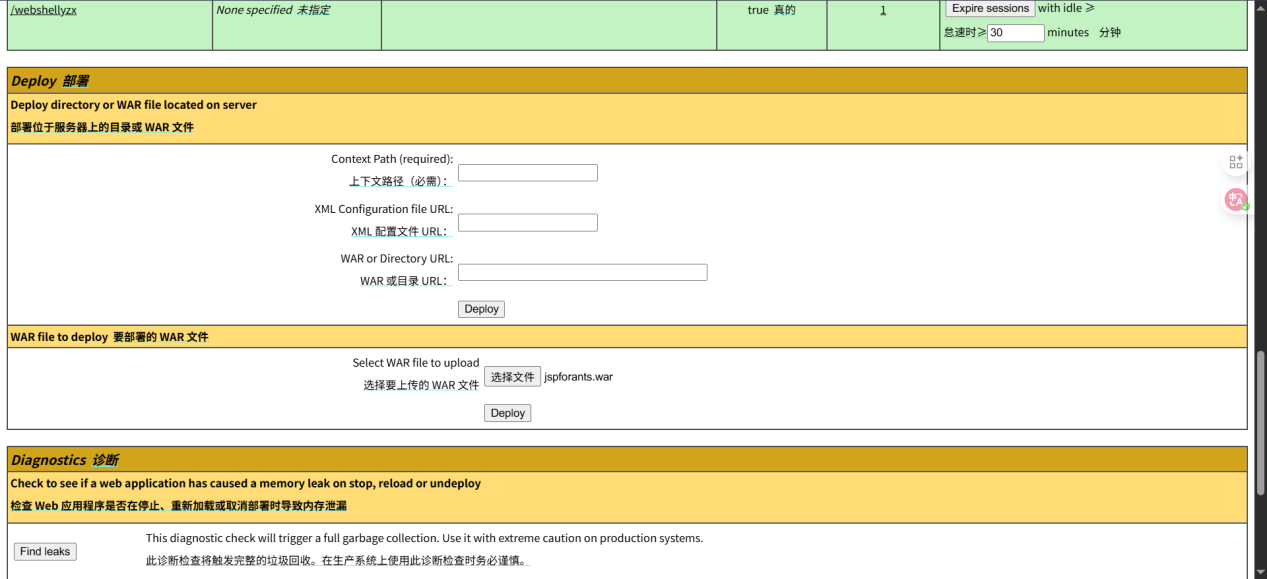
作业完成截图提交即可

1. **操作步骤**

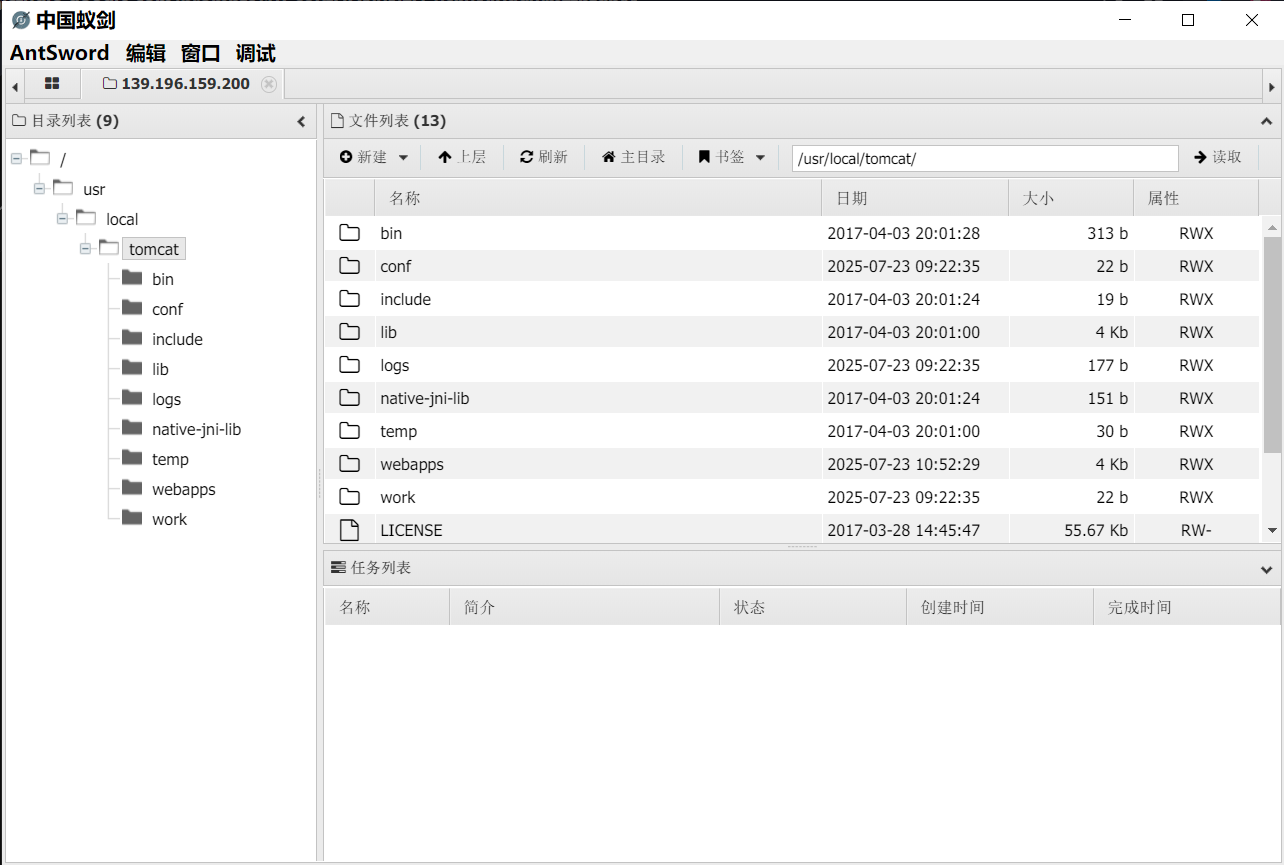
第一步：登录Tomcat后台



第二步：上传Webshell (部署WAR包)



第三步：使用蚁剑连接后门



1. **作业总结**

1.深刻认识了安全基线的重要性。 本次实验的突破口是Tomcat后台的弱口令（tomcat/tomcat）。这让我切身体会到，任何强大的系统，如果忽略了基本的安全配置，例如使用默认或过于简单的密码，就会给攻击者留下最直接的入口。这警示我们，在部署任何服务时，修改默认凭证、遵循最小权限原则是第一道，也是最关键的一道防线。

2.掌握了“后台getshell”的完整攻击链。 本次实验并非利用单一漏洞，而是演示了一条清晰的攻击链：首先通过弱口令获取认证，进入后台；然后利用后台本身合法的“WAR包部署”功能，上传恶意的Webshell程序包；最后成功获取服务器的控制权限。这个过程让我理解了攻击者如何将一个正常的管理功能转变为强大的攻击入口，学会了在渗透测试中需要将多个步骤串联，逐步扩大战果的思路。

3.熟练了渗透测试工具的实践应用。 通过本次作业，我第一次实际操作了Webshell管理工具“中国蚁剑”。我掌握了如何根据Webshell的类型（JSP）和预设的密码，来配置连接信息，并最终成功连接、获取服务器的远程文件和终端。这让我直观地感受到，掌握并善用蚁剑这类高效的自动化工具，对于在获得立足点后进行权限维持和深度渗透至关重要，极大地提升了测试效率。