weblogic漏洞

weblogic简介

WebLogic是美国Oracle公司出品的一个application server，确切的说是一个基于JAVAEE架构的中间件，WebLogic是用于开发、集成、部署和管理大型分布式Web应用、网络应用和数据库应用的Java应用服务器。将Java的动态功能和Java Enterprise标准的安全性引入大型网络应用的开发、集成、部署和管理之中。

weblogic漏洞

```
#控制台路径泄露
Weakpassword 弱口令
weblogic SSRF    (CVE-2014-4210 ) 漏洞
weblogic 反序列化 (CVE-2015-4852 )
weblogic 反序列化 (CVE-2016-0638 )
weblogic 反序列化 (CVE-2016-3510 )
weblogic 反序列化 (CVE-2017-3248 )
weblogic 反序列化 (CVE-2018-2628 )
weblogic 反序列化 (CVE-2018-2893 )
weblogic 文件上传 (CVE-2018-2894  )
weblogic XMLDecoder反序列化 (CVE-2017-10271 )
weblogic XMLDecoder反序列化 (CVE-2017-3506 )
weblogic 未授权访问CVE-2020-14883 (CVE-2020-14882)
```

Weblogic弱口令

漏洞介绍

利用后台弱口令进行登录从而getshell

漏洞原理

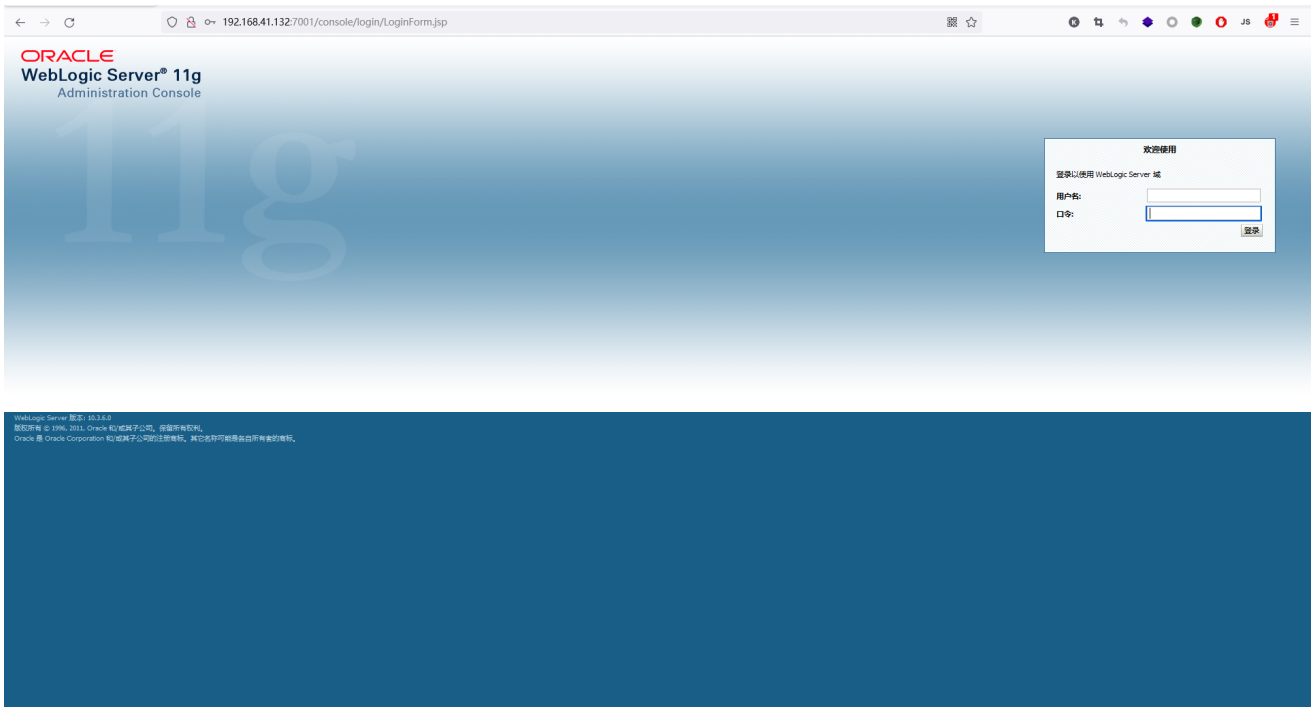
weblogic管理后台使用了弱口令

常见weblogic口令

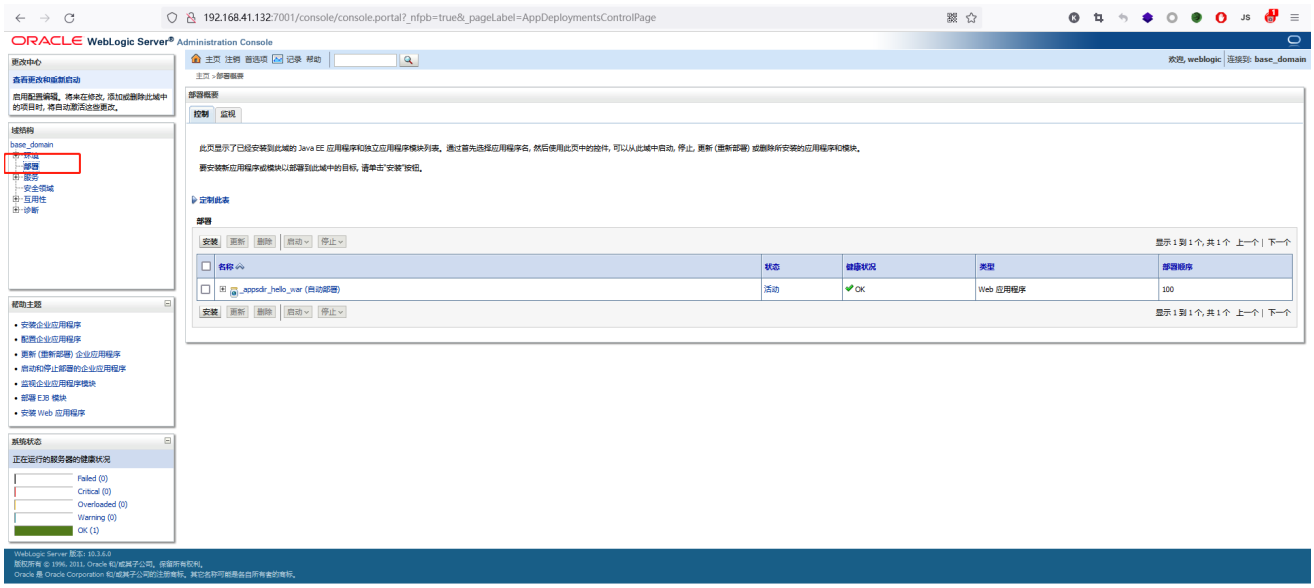
用户名	密码
system	password
weblogic	weblogic
admin	security
joe	password
mary	password
system	security
wlcsystem	wlcsystem
wlsystem	wlsystem
weblogic	Oracle@123

漏洞复现

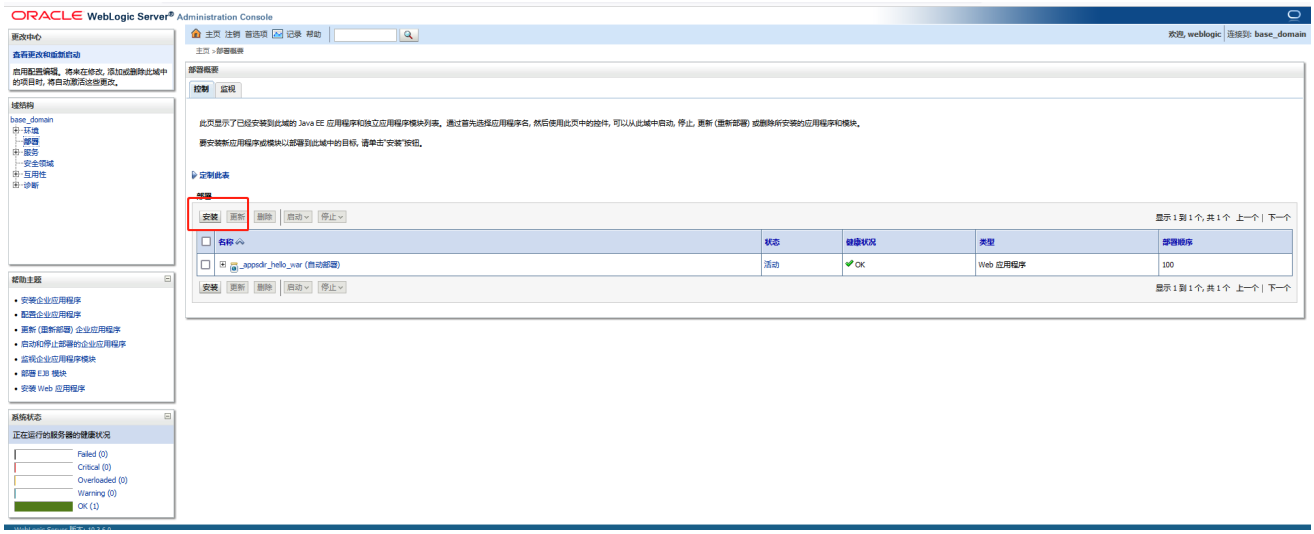
1、打开weblogic控制台`http://xxx/console`,输入weblogic/Oracle@123



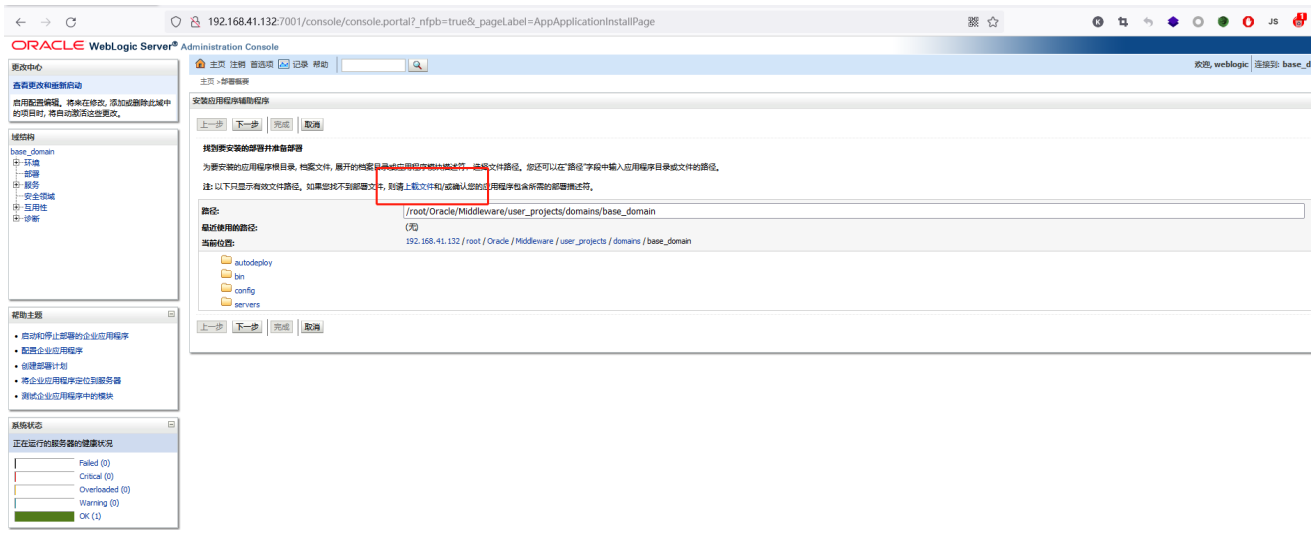
2、选择部署



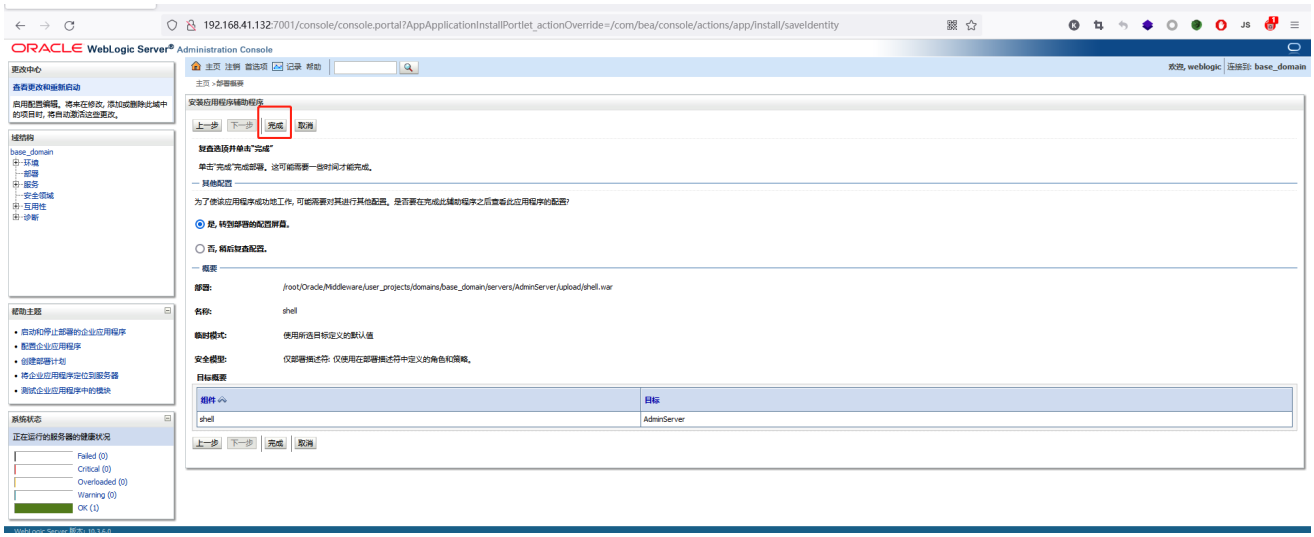
3、点击安装



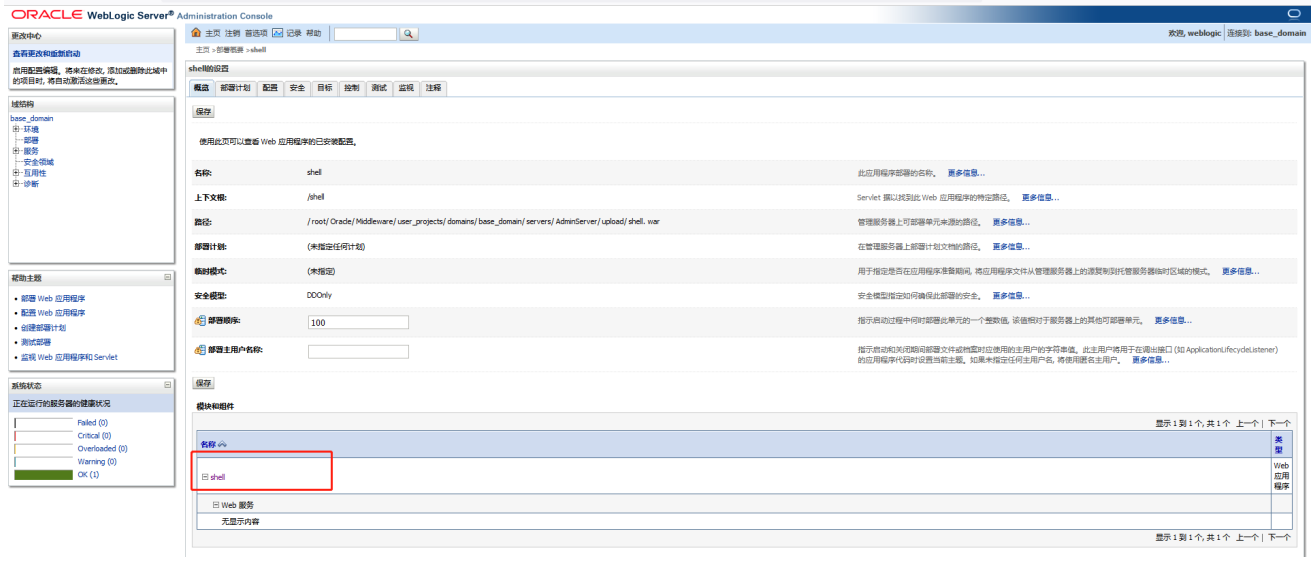
4、选择上载文件



5、制作恶意war包上穿`jar cvf shell.war shell.jsp`,选择下一步



6、步骤完成



7、访问`http://xxx/yyy/yyy.jsp`,并且连接

漏洞修复