**Weblogic任意文件上传漏洞（CVE-2018-2894）复现**

**2019-08-15**

# 前言

CNCERT持续对广泛使用的知名开源软件和商业软件进行安全缺陷分析和漏洞检测。前期发现Oracle公司出品的基于JavaEE结构的中间件WebLogic产品存在一个远程上传漏洞，并得到了厂商的确认，危害程度评分高达9.8分。鉴于近期厂商已进行了安全修复，现对漏洞情况进行简单说明。WebLogic管理端未授权的两个页面存在任意上传getshell漏洞，可直接获取权限。两个页面分别为/ws\_utc/begin.do，/ws\_utc/config.do。

**思路**

# 参考链接

<http://www.oracle.com/technetwork/security-advisory/cpujul2018-4258247.html>

<https://mp.weixin.qq.com/s/y5JGmM-aNaHcs_6P9a-gRQ>

<https://xz.aliyun.com/t/2458>

# 影响范围

Oracle WebLogic Server，版本10.3.6.0，12.1.3.0，12.2.1.2，12.2.1.3。

# 环境搭建

在这里我们使用方便快捷的docker作为漏洞的环境，由于Docker 要求 CentOS 系统的内核版本高于 3.10，所以我们使用兼容性较为完美的centos7。

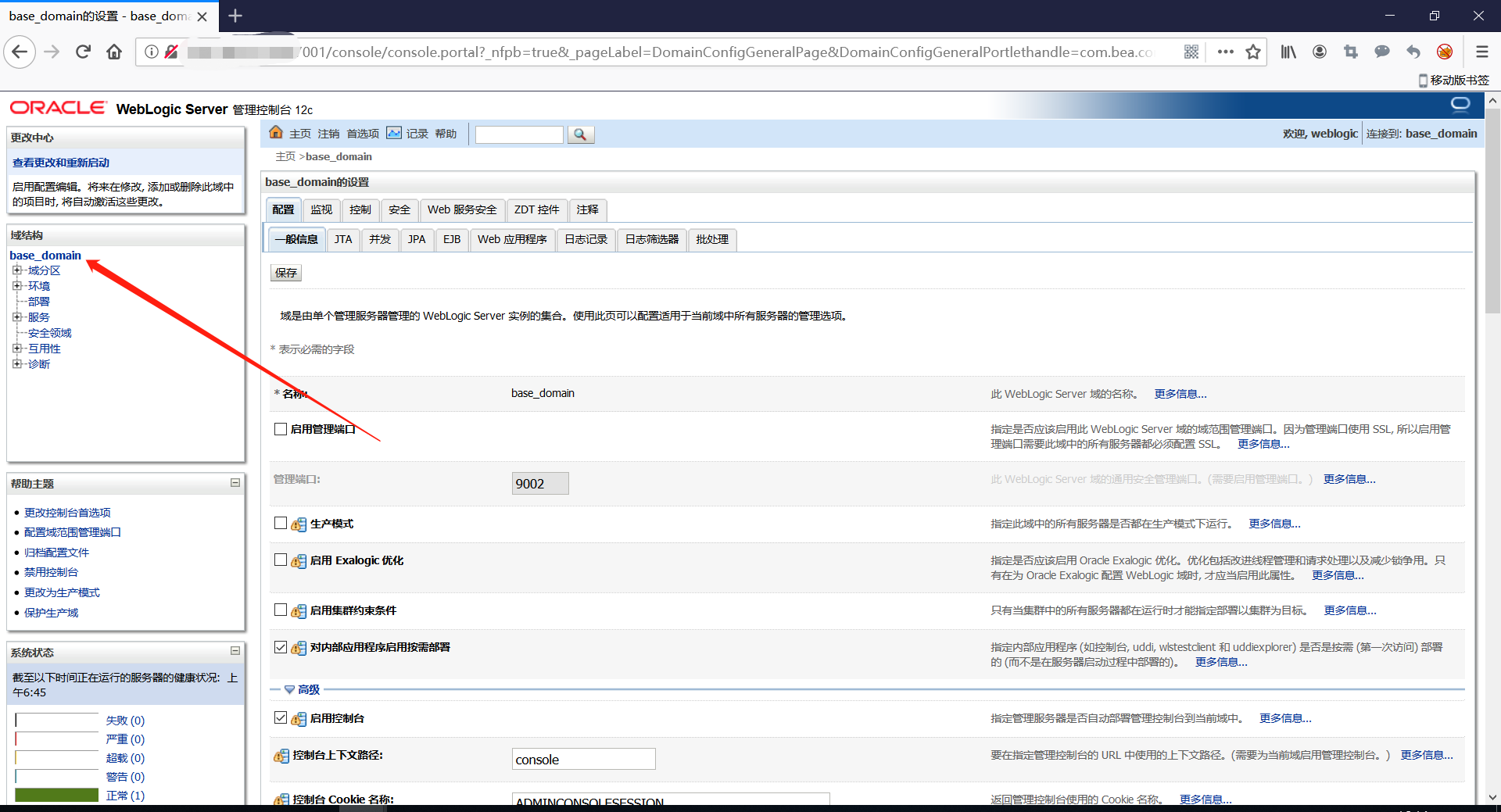
安装完成后我们直接克隆GitHub中的vulhub漏洞库即可。进入CVE-2018-2894的文件夹，执行下面的命令，启动weblogic 12.2.1.3。

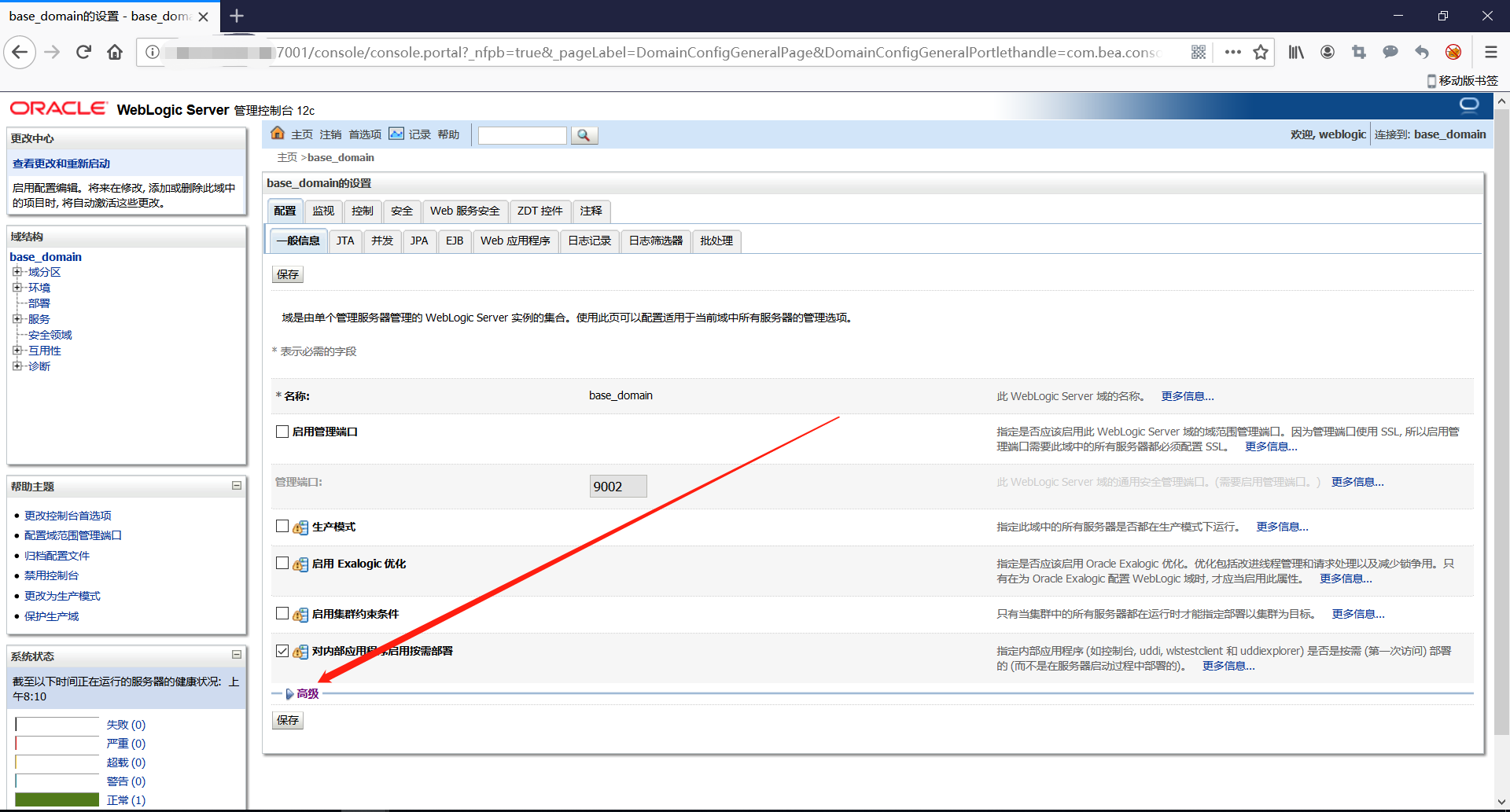
docker-compose up -d

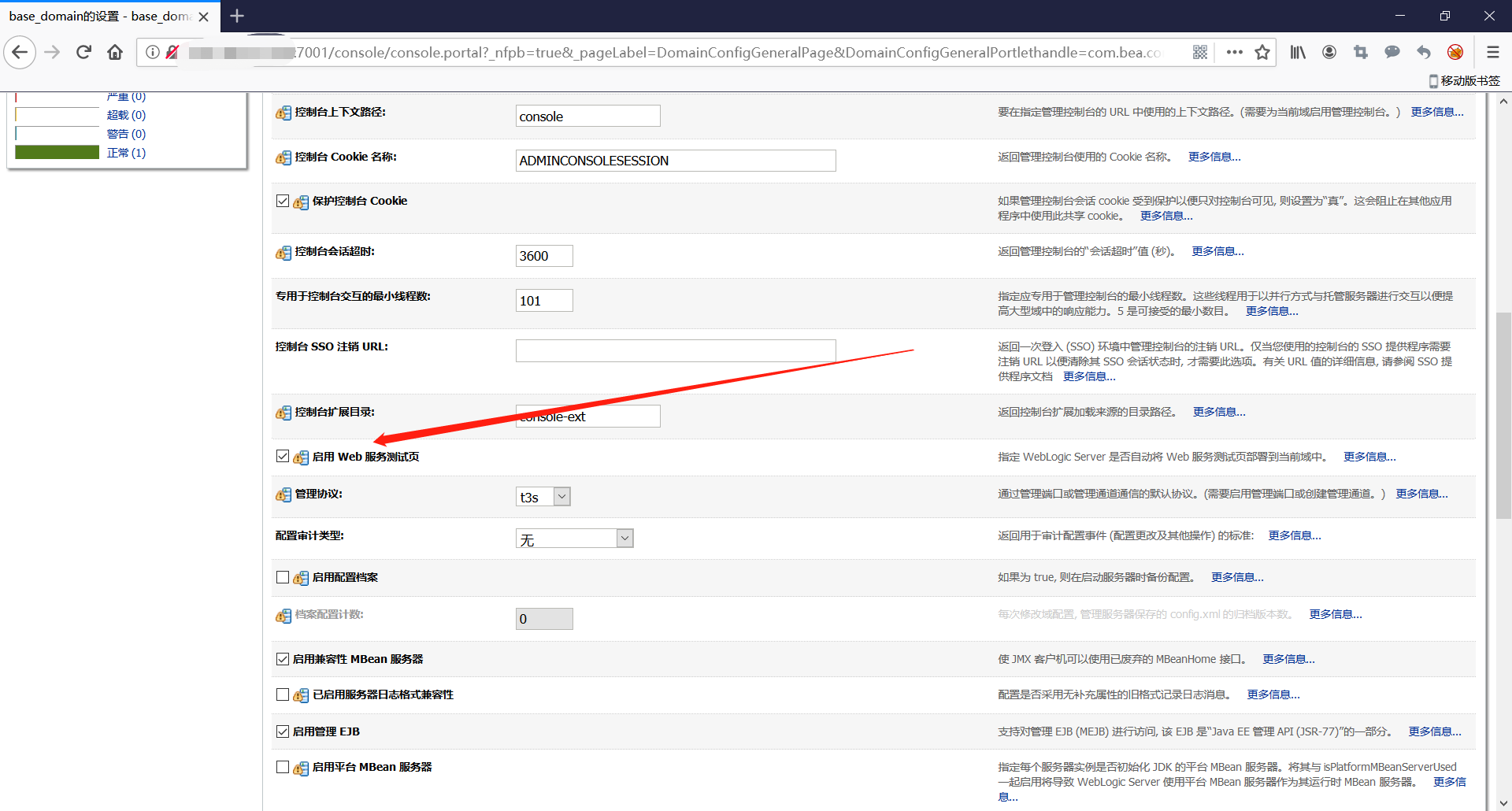
将环境启动完成后，访问http://your-ip:7001/console ，即可进入到weblogic的后台登录界面。

同时，在Linux中执行docker-compose logs | grep password 就可以查询到后台的登录密码。账号默认为weblogic。

登陆后，点击base\_domain的配置，并且在“高级”中开启“启用 Web 服务测试页”选项，如图所示



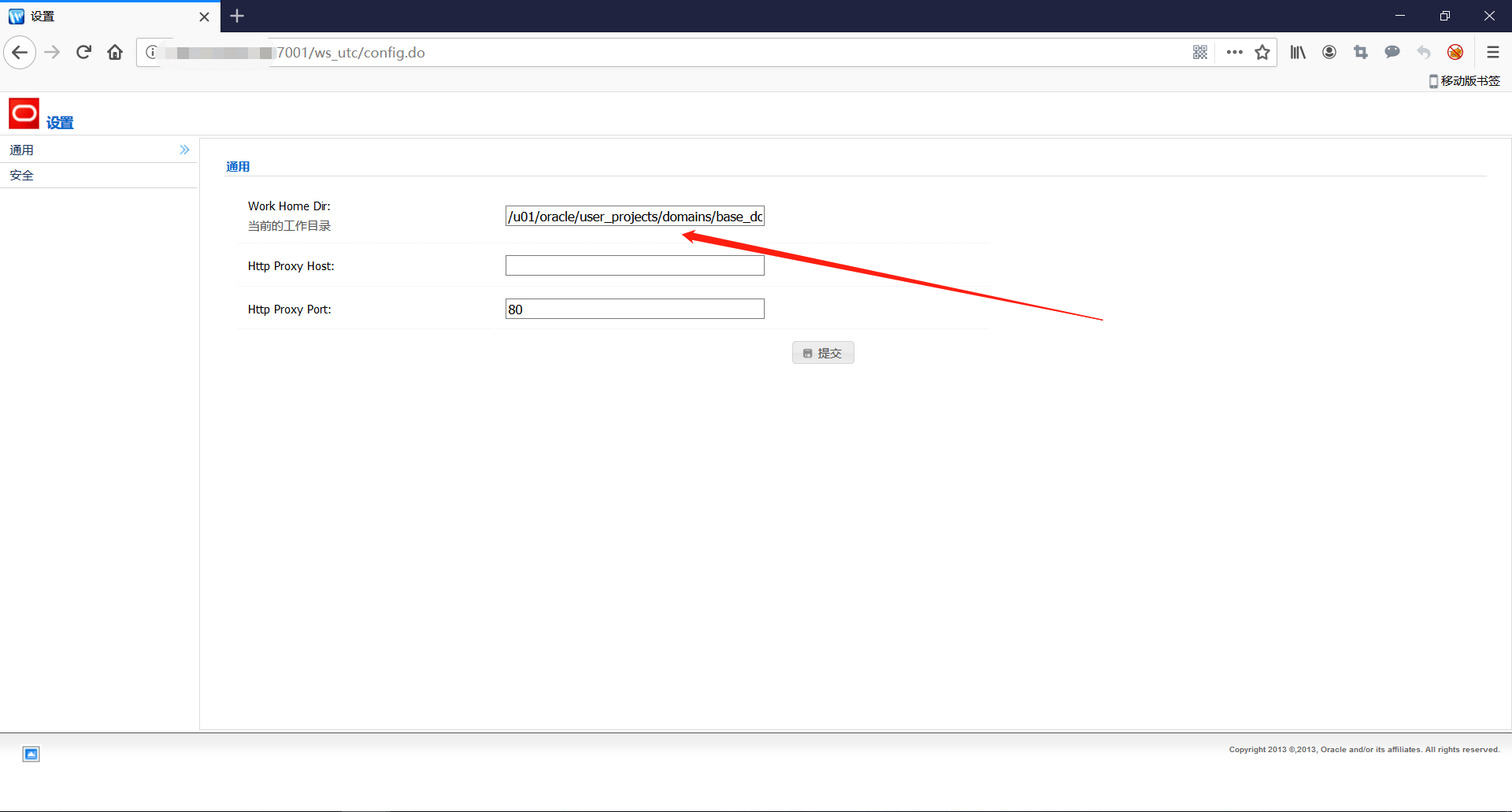




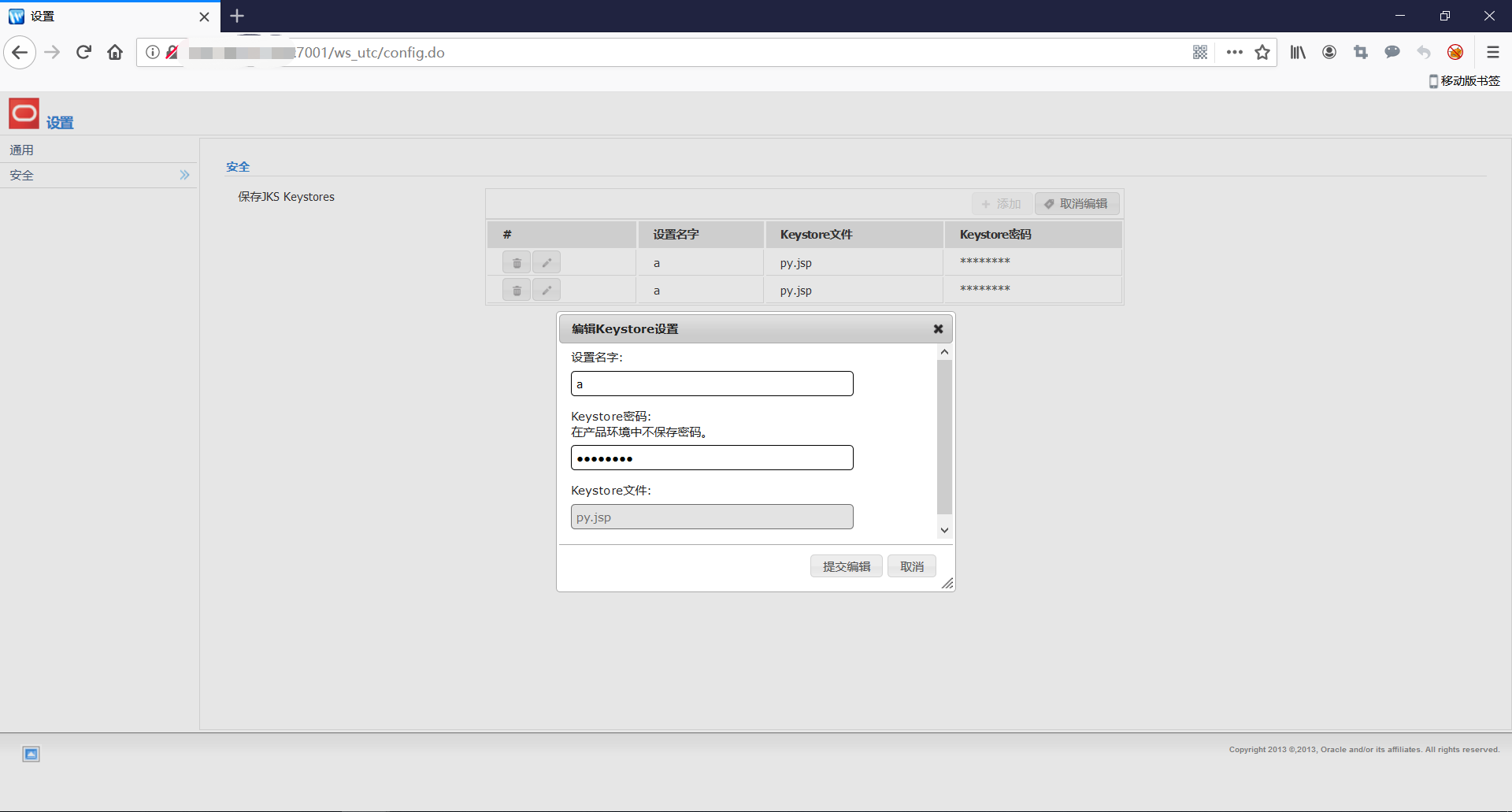
# 漏洞复现

访问http://your-ip:7001/ws\_utc/config.do，设置Work Home Dir为/u01/oracle/user\_projects/domains/base\_domain/servers/AdminServer/tmp/\_WL\_internal/com.oracle.webservices.wls.ws-testclient-app-wls/4mcj4y/war/css 。

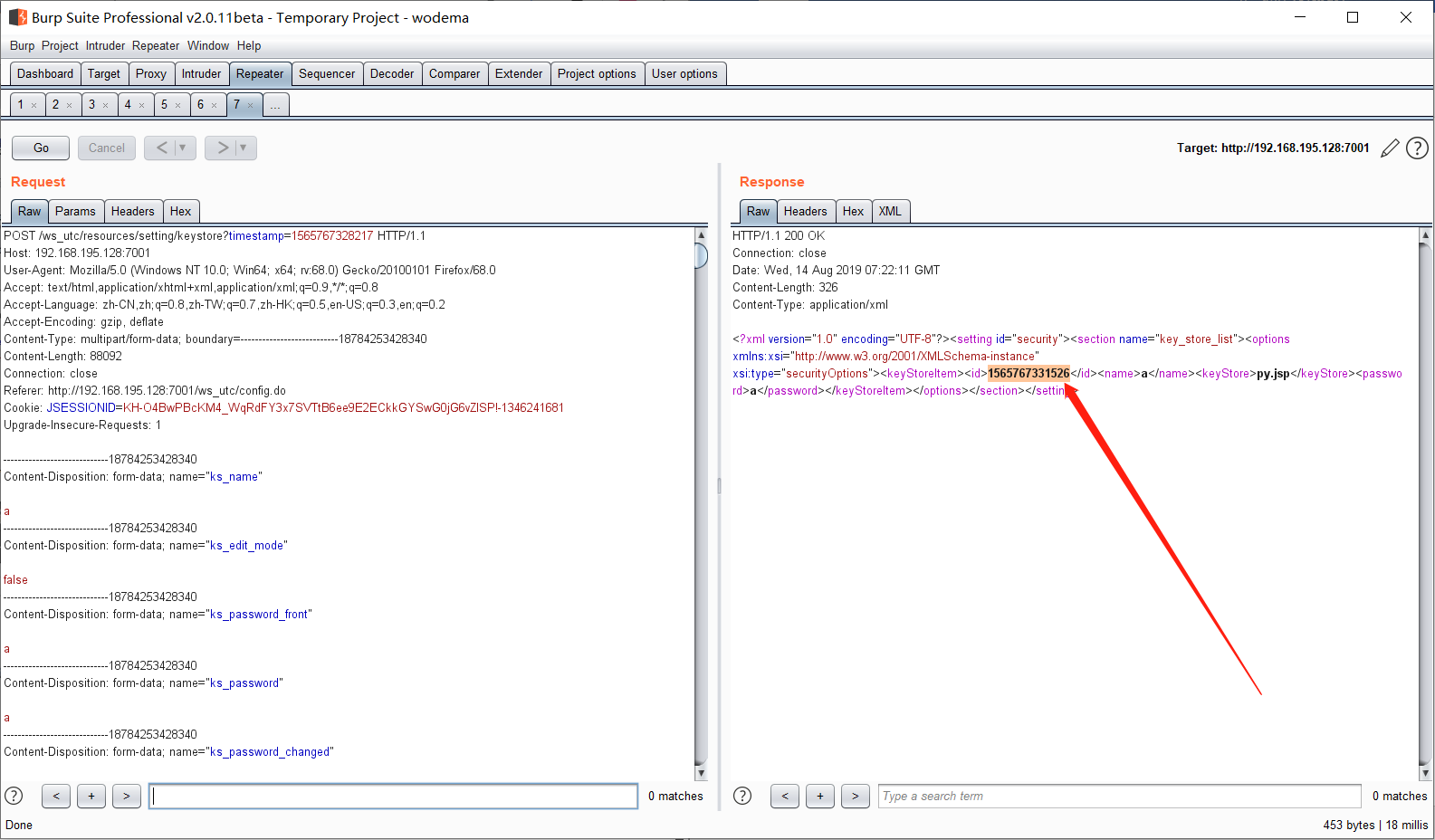
在这里我先将文件的目录设置为ws\_utc应用的静态文件css目录，访问这个目录是无需权限的，这一点很重要。



点击提交保存后切换到安全目录，点击添加，名字和密码可以自己随便设置，a/a就可以，然后点击选择文件上传webshell。



文件上传成功后，先不点击提交保存，使用抓包软件burp suite抓取数据包，查看返回的数据，会含有时间戳：



在这里我们先把这个时间戳保存下来，然后访问

http://your-ip:7001/ws\_utc/css/config/keystore/[时间戳]\_[文件名]

这样就可以直接执行webshell了：

