



WEB -



#

#

read.xxx?filename=

down.xxx?filename=

readfile.xxx?file=

downfile.xxx?file=

../ ..\ ..\ ..\

%00 ? %23 %20 .

&readpath= &filepath= &path= &inputfile= &url= &data= &readfile= &menu= META-INF= WEB-INF

1.

2.

3.

#

#Javaweb

https://blog.csdn.net/Cheng_May/article/details/78600833

<%@ page language="java" import="java.util.*" pageEncoding="UTF-8"%>

<%

String path = request.getContextPath();

String basePath = request.getScheme()+ "://" + request.getServerName() + ":" + request.getServerPort() + path + "/";

request.getScheme()+ "://" + request.getServerName() + ":" + request.getServerPort() + path + "/";

%>

public void doGet(HttpServletRequest request, HttpServletResponse response)

throws ServletException, IOException {

response.setCharacterEncoding("UTF-8");

// ContentType

response.setContentType("text/html;charset=utf-8");

//

String filename = request.getParameter("filename");

//

String folder = "/filename/";

//

```

response.addHeader("Content-type", "application/octet-stream");
response.addHeader("Content-Disposition", "attachment;filename="+filename);
//
InputStream in = getServletContext().getResourceAsStream(folder+filename);
//    response
OutputStream out = response.getOutputStream();
byte[] buffer = new byte[1024];
int len;
//
while((len = in.read(buffer)) != -1){
out.write(buffer,0,len);
}
}

```



```

Pikachu-          -

Zdns-             -

-                 -

RoarCTF2019-      -

2017    -Zone     -

-        -        -
-    WEB    WEB-INF/web.xml
-    flag    class    -
WEB-INF/classes/com/wm/ctf/FlagController.class

```



<https://www.seebug.org/vuldb/ssvid-98122>

<https://www.ichunqiu.com/battalion?t=1&r=57475>

https://blog.csdn.net/Cheng_May/article/details/78600833

<https://buuoj.cn/challenges#%5BRoarCTF%202019%5DEasy%20Java>

a
