漏洞位于:/page/exportImport/uploadOperation.jsp文件中

Jsp流程大概是:判断请求是否是multipart请求,然就没有了,直接上传了,啊哈哈哈哈哈

重点关注File file=new File(savepath+filename),

Filename参数,是前台可控的,并且没有做任何过滤限制



利用非常简单,只要对着

127.0.0.1/page/exportImport/uploadOperation.jsp

来一个multipartRequest就可以,利用简单,自评高危!!



然后请求路径:

view-source:http://112.91.144.90:5006/page/exportImport/fileTransfer/1.jsp

