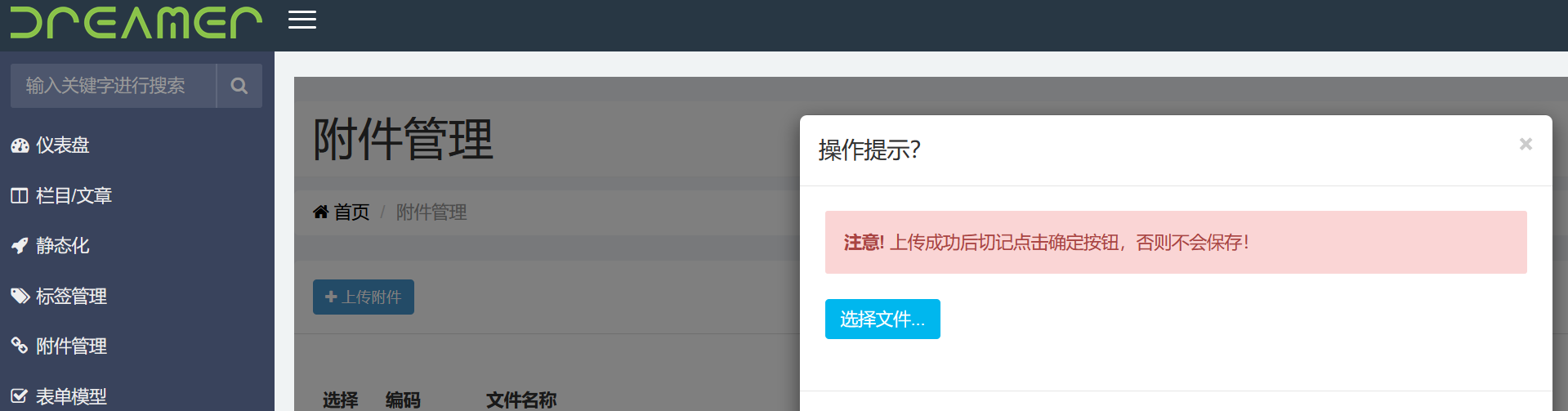
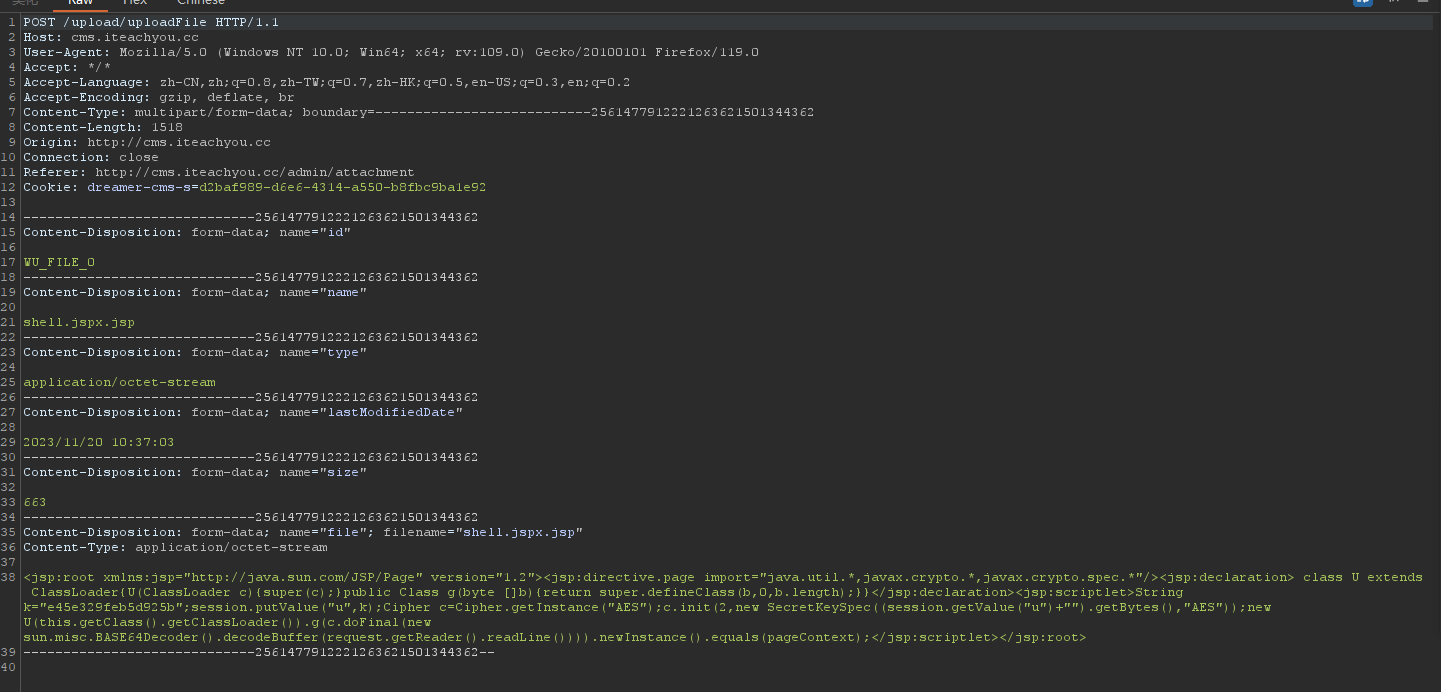
Dreamer CMS

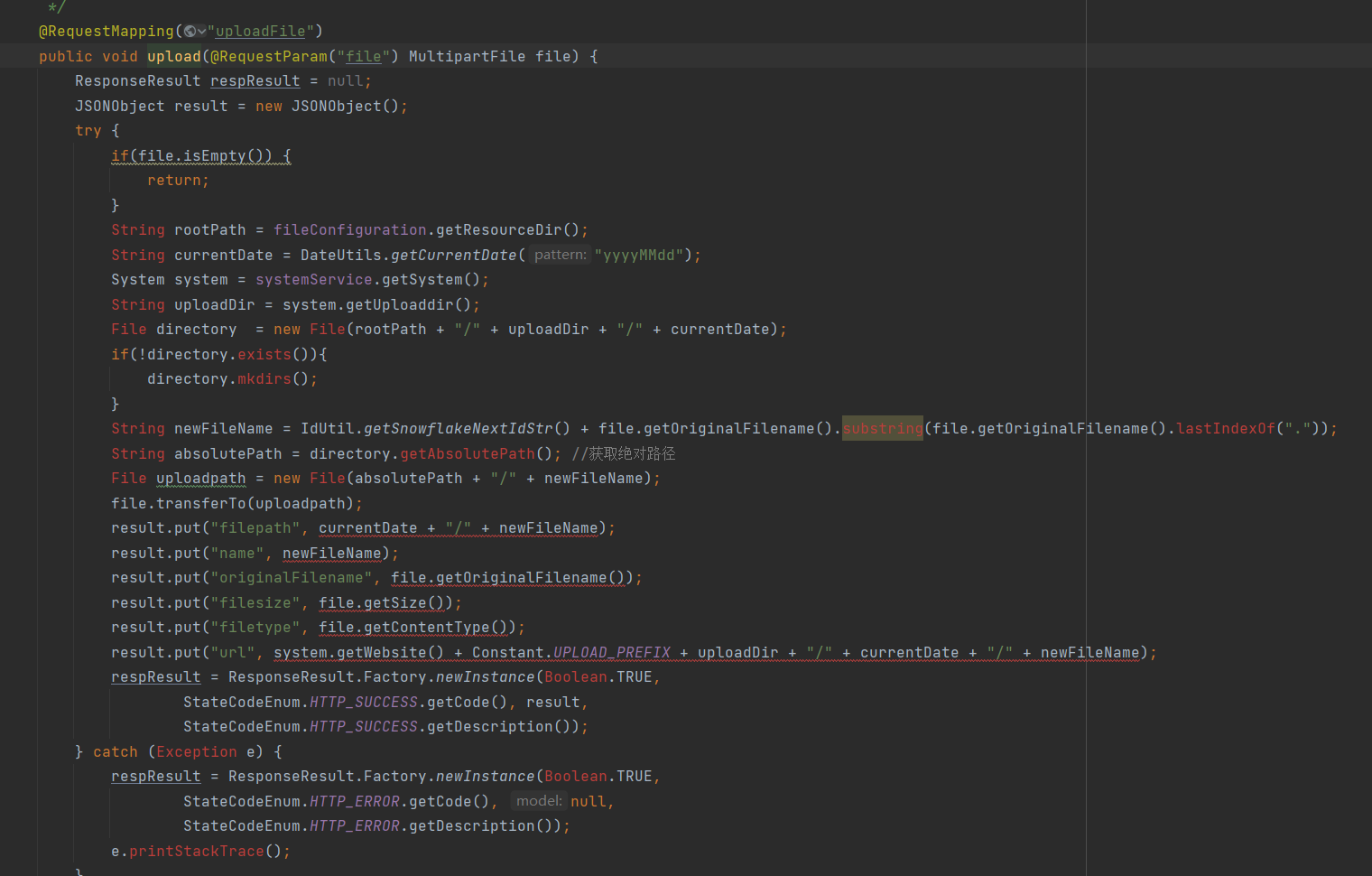
Dreamer CMS是一个梦想家内容管理系统。

任意文件上传漏洞  
Dreamer CMS 开源版V4.0.1 uploadFile存在任意文件上传，该漏洞源于组件/upload/uploadFile对用户请求未进行过滤，导致普通用户可以上传任意文件，攻击者可利用该漏洞通过注入精心设计的有效载荷执行任意Web脚本或HTML。

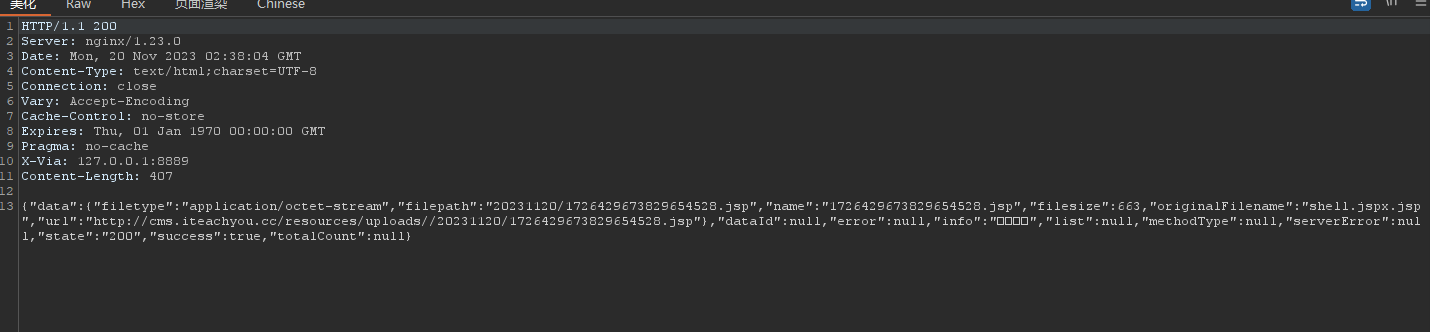




通过查看源代码发现未对后缀进行过滤导致可以上传jsp ，如下是后台源码



如下图片是上传成功之后的相应



如下图片是对url进行请求之后的响应

